Honeywell

VX7

Vehicle-Mount Computer

Microsoft® Windows® CE 5 Operating System

Reference Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

This document contains proprietary information that is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of HII.

© 2004-2012 Honeywell International Inc. All rights reserved.

Web Address: www.honeywellaidc.com

RFTerm is a trademark or registered trademark of EMS Technologies, Inc. in the United States and/or other countries.

Microsoft® Windows, ActiveSync®, MSN, Outlook®, Windows Mobile®, the Windows logo, and Windows Media are registered trademarks or trademarks of Microsoft Corporation.

Intel® and Intel XScale® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Summit Data Communications, the Laird Technologies Logo, the Summit logo, and "Connected. No Matter What" are trademarks of Laird Technologies, Inc.

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc.

Symbol® is a registered trademark of Symbol Technologies. MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.

Wavelink®, the Wavelink logo and tagline, Wavelink Studio™, Avalanche Management Console™, Mobile Manager™, and Mobile Manager Enterprise™ are trademarks of Wavelink Corporation, Kirkland.

RAM® and RAM Mount™ are both trademarks of National Products Inc., 1205 S. Orr Street, Seattle, WA 98108.

Acrobat® Reader © 2012 with express permission from Adobe Systems Incorporated.

Other product names or marks mentioned in this document may be trademarks or registered trademarks of other companies and are the property of their respective owners.

Patents

For patent information, please refer to www.honeywellaidc.com/patents.

Limited Warranty

Refer to www.honeywellaidc.com/warranty_information for your product’s warranty information.

Table of Contents

Chapter 1: Introduction 1-1

End User License Agreement (EULA) 1-1

Reboot 1-2

Warmboot 1-2

Coldboot 1-2

Components 1-3

Top View 1-3

Front View 1-3

Bottom View 1-4

Back View 1-4

Control Panel 1-5

Access Panel 1-5

Chapter 2: Hardware 2-7

System Hardware 2-7

802.11b/g and a/b/g Wireless Client 2-8

Central Processing Unit 2-8

Input/Output Components 2-8

System Memory 2-8

Video Subsystem 2-8

Power Supply 2-9

Uninterruptible Power Supply 2-9

Backup Battery 2-9

Audio Interface 2-9

Card Slots 2-9

PCMCIA Slots 2-9

CompactFlash (CF) Slot 2-9

Secure Digital (SD) Slot 2-9

Bluetooth LXEZ Pairing 2-10

Power Modes 2-11

On Mode 2-11

User Idle Mode 2-11

Primary Events 2-11

Suspend Mode 2-11

Off Mode 2-11

External Connectors 2-12

Scanner Serial Connector (COM1) 2-13

Printer / PC Serial Connector (COM3) 2-14

Technical Specifications - Connection Cable 2-15
RTS/CTS Handshaking and the Serial Port 2-15
Screen Blanking Cable 2-16
Serial Cable 2-16
Sample Cable for Screen Blanking 2-17
PS/2 Keyboard/Mouse 2-18
USB Keyboard / Mouse 2-18
Keyboard / Mouse Connector 2-18
PS/2 Keyboard / Mouse Cable 2-19
D9 Male Connector 2-19
PS/2 Keyboard Connector 2-20
PS/2 Mouse Connector 2-20
USB and Optional Ethernet Connector 2-21
Ethernet / USB Dongle Cables 2-22
D15 Female Connector 2-23
USB Host Connector 2-24
USB Client Connector 2-24
RJ45 Connector 2-25
Audio Connector 2-26
Power Supply Connector 2-26
UPS Battery Pack Connectors 2-27
Input Connector Pinout 2-27
Output Connector Pinout 2-27
UPS Battery Extension Cable Connector 2-28
Input Connector Pinout 2-28
Output Connector Pinout 2-28
Antenna Connections 2-29
Spread Spectrum RF Antenna Connector Pin 2-29
Vehicle Remote Antenna Mount 2-29
Internal Antenna 2-30
User Access Panel 2-31
Remove User Access Panel Cover 2-31
Inside the User Access Panel 2-31
Reinstall User Access Panel Cover 2-32
QWERTY 95 Key Keyboard 2-33
Keyboard Indicators 2-33
Numlock 2-33
CapsLock 2-34
Scroll Lock 2-34
Keyboard Backlight 2-34

QWERTY Keyboard 2-35
IBM 3270 Overlay 2-35
IBM 5250 Overlay 2-36
Keyboard LEDs 2-36
CAPS LED 2-37
Secondary Keys LED 2-37
Control Keys 2-38
LED Functions 2-39
Status LED 2-39
60 Key Keyboard - Keyboard LEDs 2-39
Speakers 2-39
Display 2-40
Touch Screen 2-40
Touch Screen Heater 2-40
Power Supply 2-41
External Power Supply 2-41
Fuse 2-42
Chapter 3: Software 3-1
Introduction 3-1
Operating System 3-1
Windows CE Operating System 3-1
General Windows CE Keyboard Shortcuts 3-2
Warmboot 3-3
Coldboot 3-3
Clearing Persistent Storage / Reset to Default Settings 3-3
Folders Copied at Startup 3-3
Saving Changes to the Registry 3-4
Software Load 3-5
Software Applications 3-5
ActiveSync 3-5
Bluetooth (Optional) 3-5
Java (Optional) 3-5
RFTerm (Optional) 3-6
Avalanche 3-6
Software Development 3-6
Access Files on the CF/SD Card 3-6
VX7 Utilities 3-7
LAUNCH.EXE 3-7
LAUNCH.EXE and Persistent Storage 3-9

REGEDIT.EXE 3-9
REGLOAD.EXE 3-9
REGDUMP.EXE 3-9
WARMBOOT.EXE 3-9
WAVPLAY.EXE 3-9
VX7 Command-line Utilities 3-10
COLDBOOT.EXE 3-10
PrtScrn.EXE 3-10
Desktop 3-11
Desktop Icons 3-11
Taskbar 3-12
My Device Folders 3-12
Wavelink Avalanche Enabler (Optional) 3-13
Internet Explorer 3-13
Start Menu Program Options 3-14
Communication 3-15
ActiveSync 3-15
Start FTP Server / Stop FTP Server 3-15
Summit 3-15
Certs 3-15
Command Prompt 3-16
eXpress Scan 3-16
Internet Explorer 3-16
Media Player 3-17
Microsoft File Viewers 3-17
Microsoft WordPad 3-17
Remote Desktop Connection 3-17
Settings 3-18
Transcriber 3-18
Windows Explorer 3-18
Taskbar 3-19
General Tab 3-19
Advanced Tab 3-19
Expand Control Panel 3-19
Clear Contents of Document Folder 3-20
Taskbar Icons 3-20
VX7 OS Upgrade 3-21
Introduction 3-21
Preparation 3-21
Procedure 3-21

ActiveSync 3-22
Introduction 3-22
Initial Setup 3-22
Connect via USB 3-23
Cables for USB ActiveSync Connection: 3-23
Serial Connection 3-24
Cable for Serial ActiveSync Connection 3-24
Wireless Connection 3-24
VX7 with Disabled Touch Screen 3-25
Synchronizing from the Mobile Device 3-25
Explore 3-25
Backup Data Files using ActiveSync 3-25
Prerequisites 3-25
Serial Port Transfer 3-25
USB Transfer 3-25
Connect 3-26
Disconnect 3-26
Cold Boot and Loss of Host Re-connection 3-26
ActiveSync Help 3-27
Configuring the VX7 with LXEConnect 3-28
Install LXEConnect 3-28
Using LXEConnect 3-30
Control Panel 3-32
About 3-34
Version Tab and the Registry 3-34
Language and Fonts 3-34
Identifying Software Versions 3-35
MAC Address 3-35
Accessibility 3-36
Administration - AppLock 3-37
Setup a New Device 3-38
Administration Mode 3-38
End User Mode 3-39
Passwords 3-39
End-User Switching Technique 3-40
Using a Stylus Tap 3-40
Using the Switch Key Sequence 3-40
Hotkey (Activation hotkey) 3-41
Application Configuration 3-42
Application Panel 3-42

Launch Button 3-43
Auto At Boot 3-44
Auto Re-Launch 3-45
Manual (Launch) 3-46
Allow Close 3-46
Match 3-47
End User Internet Explorer (EUIE) 3-47
Security Panel 3-48
Hotkey 3-48
Password 3-48
Options Panel 3-49
Launch timeout 3-49
Replace timeout 3-49
Restart timeout 3-49
Status Panel 3-49
View 3-50
Log 3-50
Save As 3-50
AppLock Help 3-51
AppLock Error Messages 3-51
Bluetooth 3-59
Bluetooth Devices 3-60
Discover 3-61
Stop Button 3-61
Bluetooth Device List 3-62
Clear Button 3-62
Bluetooth Device Menu 3-63
Right Click Menu Options 3-63
Bluetooth Device Properties 3-64
Settings 3-65
Turn Off Bluetooth 3-65
Options 3-66
Reconnect 3-67
Options 3-68
OPP Setup 3-70
OPP Send 3-72
Buttons 3-72
About 3-73
Using Bluetooth 3-74
Bluetooth Devices Display - Before Discovering Devices 3-74

Initial Configuration 3-74
Subsequent Use 3-75
Bluetooth Indicators 3-76
Bluetooth Barcode Reader Setup 3-76
Prerequisites 3-76
VX7 with Label 3-77
VX7 without Label 3-77
Bluetooth Beep and LED Indications 3-79
Bluetooth Printer Setup 3-79
Easy Pairing and Auto-Reconnect 3-79
Using OPP 3-80
Pairing with an OPP Device 3-80
Remote Device Pushes File to VX7 3-80
VX7 Pushes File to Remote Device 3-81
LXEZ Pairing and External Application 3-81
Certificates 3-82
Date / Time 3-83
Device Management 3-84
Dialing 3-85
Display 3-86
Background 3-86
Appearance 3-86
Backlight 3-87
Input Panel 3-88
Installed Programs 3-89
Internet Options 3-90
Keyboard 3-93
KeyPad 3-94
KeyMap Tab 3-95
Remap a Single Key 3-95
Remap a Key to a Unicode Value 3-95
Remap a Key Sequence 3-95
Remap a Key to a Sequence of Unicode Values 3-96
Remap an Application 3-96
Remap a Command 3-96
LaunchApp Tab 3-98
RunCmd Tab 3-99
License Viewer 3-100
Mixer 3-101
Mouse 3-102

MX3X-VXC Options 3-103
Communication 3-103
Enable TCP/IP Version 6 3-103
Allow Remote Desktop Autologon 3-103
Autolaunch TimeSync 3-103
Disable SNMP 3-104
LXE BTRS Enabled 3-104
Misc 3-105
CapsLock 3-105
NumLock 3-105
Touch Screen Disable 3-105
Touch Screen Heater Disable 3-105
Screen Size 640x480 3-105
Large SIP 3-105
Enable RFTerm Auto Launch 3-106
Enable Auto Launch IP Wait 3-106
IP Wait Timeout 3-106
Status Popup 3-107
Network and Dialup Options 3-108
Create a New Connection 3-108
Network Capture 3-109
Netlog 3-109
NDISLog 3-111
Owner 3-112
Password 3-114
PC Connection 3-115
PCMCIA 3-116
PCMCIA 1 3-116
PCMCIA 2 3-117
IntATA Tab Options 3-117
Power 3-118
Regional and Language Settings 3-120
Remove Programs 3-122
Scanner 3-123
Bar Code Readers 3-123
Return to Factory Default Settings 3-123
Barcode Processing Overview 3-123
Factory Default Settings 3-124
Main Tab 3-125
Screen Blanking 3-126

Technical Specifications - Screen Blanking Cable 3-127
Serial cable 3-127
Pinout 3-127
COM1 Tab 3-128
COM3 Tab 3-129
Serial Port Pin 9 3-130
Enable Handshaking 3-130
Barcode Tab 3-131
Buttons 3-131
Enable Code ID 3-132
Options 3-132
Notes 3-132
Barcode – Custom Identifiers 3-133
Parameters 3-133
Name text box 3-133
ID Code text box 3-133
Buttons 3-134
Add 3-134
Insert 3-134
Edit 3-134
Clear All 3-134
Remove 3-134
Control Code Replacement Examples 3-134
Barcode Processing Examples 3-135
Barcode - Ctrl Char Mapping 3-136
Translate All 3-136
Parameters 3-136
Barcode - Symbology Settings 3-137
Parameters 3-138
Strip Leading/Trailing Control 3-139
Barcode Data Match List 3-139
Barcode Data Match Edit Buttons 3-140
Match List Rules 3-140
Add Prefix/Suffix Control 3-141
Length Based Barcode Stripping 3-141
Hat Encoding 3-144
Stylus 3-146
System 3-147
General Tab 3-147
Memory Tab 3-148

Device Name Tab 3-148
Copyrights Tab 3-149
Terminal Server Client Licenses 3-150
Volume and Sounds 3-151
Good Scan and Bad Scan Sounds 3-152
WiFi 3-153
Chapter 4: Enabler Installation and Configuration 4-1
Introduction 4-1
Installation 4-1
Installing the Enabler on Mobile Devices 4-1
VX6/VX7 Enabler Installation 4-2
Enabler Uninstall Process 4-2
Stop the Enabler Service 4-2
Update Monitoring Overview 4-4
Mobile Device Wireless and Network Settings 4-5
Preparing a Device for Remote Management 4-6
Using Wavelink Avalanche to Upgrade System Baseline 4-7
Part 1 – Bootstrapping the RMU 4-7
Part 2 – Installing Packages 4-7
Version Information on Mobile Devices 4-7
User Interface 4-8
Enabler Configuration 4-8
File Menu Options 4-10
Avalanche Update using File > Settings 4-11
Menu Options 4-11
Connection 4-12
Server Contact 4-13
Data 4-14
Preferences 4-15
Display 4-17
Taskbar 4-18
Execution 4-19
Scan Config 4-20
Shortcuts 4-21
SaaS 4-22
Adapters 4-23
Status 4-26
Startup/Shutdown 4-27
Exit 4-28

Using Remote Management 4-28
Using eXpress Scan 4-29
Step 1: Create Bar Codes 4-29
Step 2: Scan Bar Codes 4-29
Step 3: Process Completion 4-31
Chapter 5: Wireless Network Configuration 5-1
Important Notes 5-1
Summit Client Utility 5-2
Help 5-2
Summit Tray Icon 5-2
Wireless Zero Config Utility and the Summit Radio 5-3
How To: Use the Wireless Zero Config Utility 5-3
How to: Switch Control to SCU 5-3
Main Tab 5-4
Auto Profile 5-5
Admin Login 5-5
Profile Tab 5-7
Buttons 5-8
Profile Parameters 5-9
Status Tab 5-11
Diags Tab 5-12
Global Tab 5-13
Custom Parameter Option 5-14
Global Parameters 5-15
Sign-On vs. Stored Credentials 5-19
How to: Use Stored Credentials 5-19
How to: Use Sign On Screen 5-19
Windows Certificate Store vs. Certs Path 5-20
User Certificates 5-20
Root CA Certificates 5-20
How To: Use the Certs Path 5-21
How To: Use Windows Certificate Store 5-21
Configuring the Profile 5-21
No Security 5-23
WEP 5-24
LEAP 5-25
PEAP/MSCHAP 5-26
PEAP/GTC 5-28
WPA/LEAP 5-30

EAP-FAST 5-32
EAP-TLS 5-34
WPA PSK 5-36
Certificates 5-37
Generating a Root CA Certificate 5-37
Installing a Root CA Certificate 5-40
Generating a User Certificate 5-41
Installing a User Certificate 5-46
Verify Installation 5-49
Chapter 6: Keymaps 6-1
95 Key KeyMap 101-Key Equivalencies 6-1
60 Key KeyMap 101-Key Equivalencies 6-2
IBM Terminal Emulation 6-7
IBM 3270 6-7
IBM 5250 6-8
Chapter 7: Technical Specifications 7-1
VX7 7-1
Dimensions 7-2
Environmental Specifications 7-2
VX7 7-2
UPS Battery Pack 7-2
Network Card Specifications 7-3
Summit 802.11 b/g CF 2.4GHz 7-3
Summit 802.11a/b/g CF 2.4/5.0GHz 7-3
Bluetooth 7-3
Chapter 8: Technical Assistance 8-1

Chapter 1: Introduction

The VX7 Vehicle Mount Computer (VMC) is a rugged, vehicle mounted, PC (Personal Computer) running a Microsoft® Windows® CE operating system and capable of wireless data communications from a fork-lift truck or any properly configured vehicle.

The optional Bluetooth® module supports Bluetooth printers and scanners. The VX7 provides the power and functionality of a desktop computer in a vehicle mounted unit, with a wide range of options.

Contact Technical Assistance for information on the latest upgrades for your VX7.

End User License Agreement (EULA)

When a new VX7 starts up a EULA is displayed on the touch screen. It remains on the screen until the Accept or Decline button is tapped with a stylus.

Tap the Accept button to accept the EULA terms and the VX7 continues the startup process. The EULA is not presented to the user again.

Tap the Decline button to decline the EULA and the VX7 will reboot. It will continue to reboot until the Accept button is tapped with the stylus.

Note: The EULA will be presented after any operating system upgrade or re-installation, including language-specific operating systems.

Reboot

When the Windows CE desktop is displayed or an application begins, the power up (or reboot) sequence is complete.

Warmboot

A warmboot reboots the computer without erasing any registry data. However, any applications installed to RAM are lost, as is all data in RAM. This occurs because the operating system is stored on the flash drive, but must be loaded into RAM to run.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System folder and configured in the Registry to persist are reinstalled on boot up by the Launch utility.

To warmboot the VX7, select **Start > Run** and type

```
warmboot
```

and tap the **OK** button.

Coldboot

A coldboot reboots the computer, erases all registry data and returns the computer to factory default settings. In order to be preserved, applications and data must be stored in the System folder. Registry information is not preserved. Only factory default applications and drivers stored as .CAB files in the System folder are loaded by Launch.

A coldboot is initiated by running the Coldboot application in the Windows folder. This application automatically cold boots the VX7, erasing any customer applied registry changes and returning the VX7 to its factory settings.

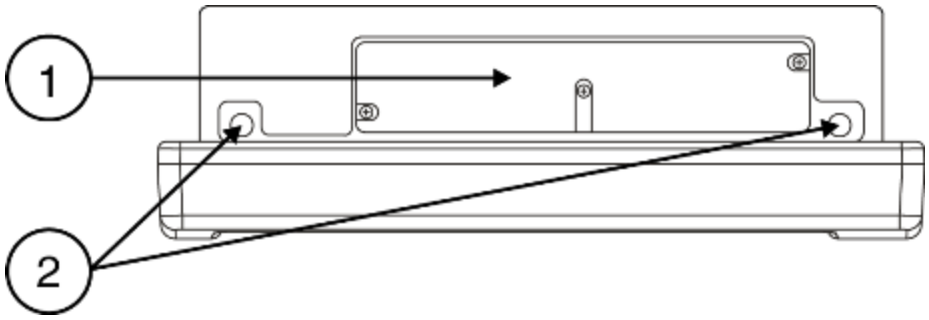
To coldboot the VX7, select **Start > Run** and type

```
coldboot
```

and tap the **OK** button.

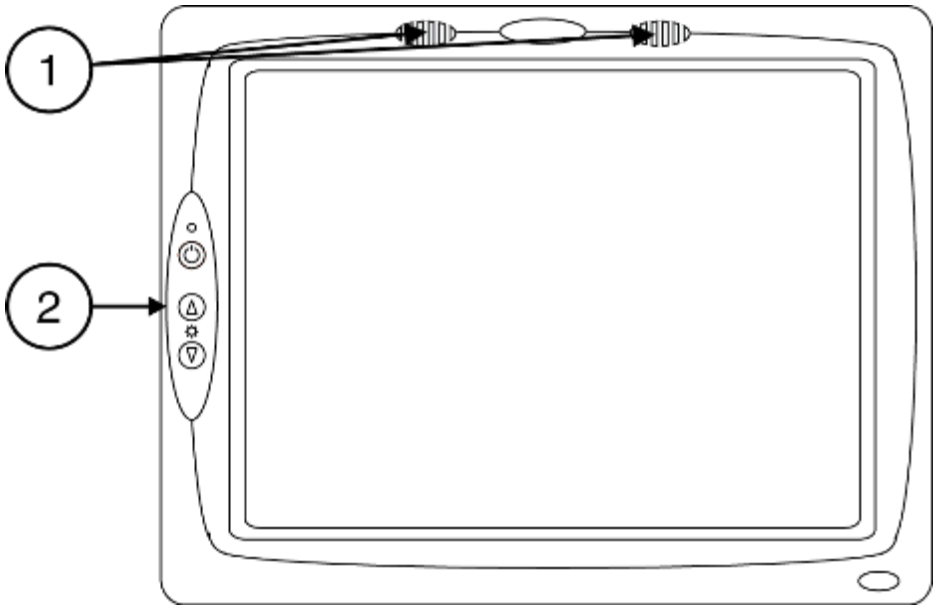
Components

Top View



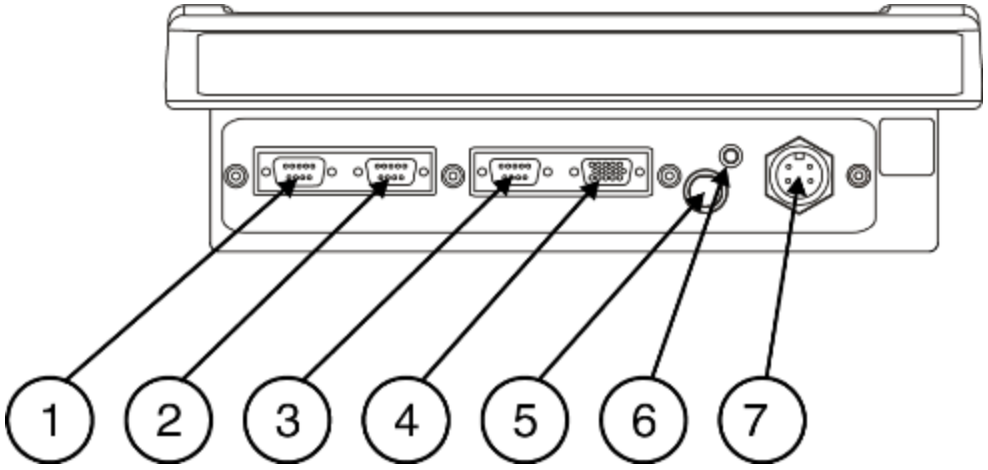
1. Access Panel Cover
2. Antenna Connectors or Hole Plugs

Front View



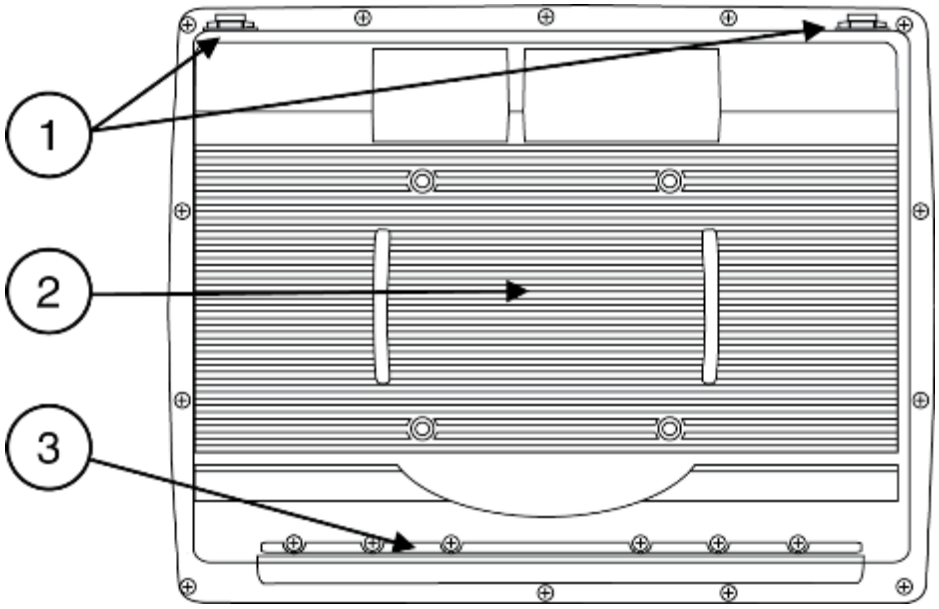
1. Speakers
2. Control Panel

Bottom View



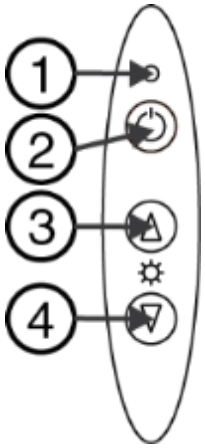
1. COM1/Scanner Connector
2. COM3 Connector
3. Keyboard/Mouse Connector (Not Used)
4. Ethernet/USB Cable Connector (USB-Host and USB-Client
5. Fuse
6. Audio Connector
7. Power Cable Connector

Back View



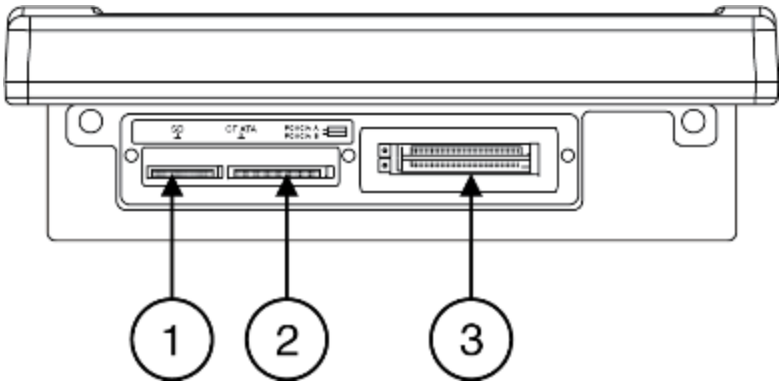
1. Antenna Connectors
2. Bracket Mounting Area
3. Strain Relief Bracket and Screws

Control Panel



1. Status / Power LED
2. Power Switch
3. Brightness Increase
4. Brightness Decrease

Access Panel

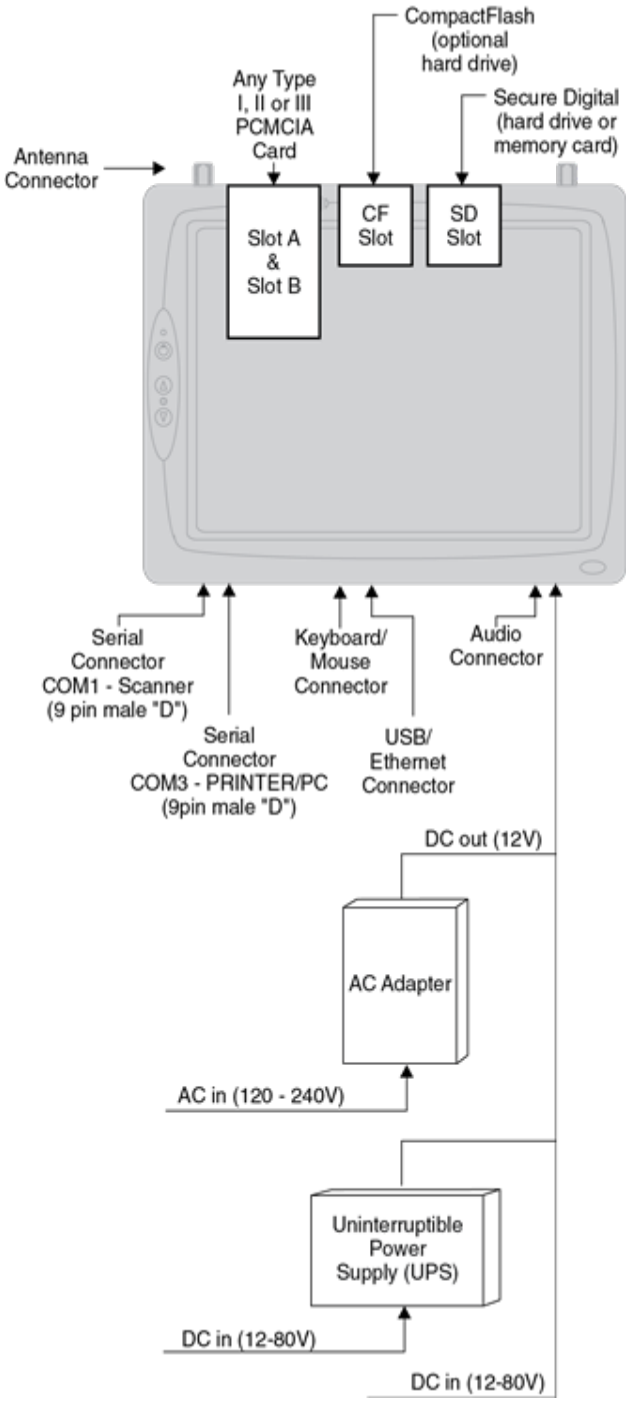


1. SD Memory Card Slot
2. CompactFlash Hard Drive
3. PCMCIA Slots

Note: The tethered access panel cover is not shown in the illustration above.

Chapter 2: Hardware

System Hardware



802.11b/g and a/b/g Wireless Client

The VX7 has an 802.11x network card that supports diversity with two antennas. The CPU board does not allow hot swapping the network card. Power management for the network card is configured with the Summit Client Utility.

WEP, WPA and LEAP are supported.

Central Processing Unit

The CPU is a 400MHz Intel PXA255. The operating system is Microsoft Windows CE. The OS image is stored on an internal SD flash card and is loaded into DRAM for execution.

Input/Output Components

The VX7 supports the following I/O components of the core logic:

- Two 9-pin RS-232 serial ports configured as COM1 and COM3 (labeled "COM2/3"). There is no COM2 port on the VX7.
- Two PCMCIA slots (supporting Type I or II PCMCIA cards).
- One slot for SD memory card.
- CompactFlash (CF) or Secure Digital (SD) drive.
- VMT or standard PS/2 keyboard (via a watertight connector).
- Ports available via dongle cable:
  - USB Host port
  - USB Client port
  - optional Ethernet port
- One audio jack providing monaural audio output.

System Memory

Main system memory is 128MB DRAM.

Video Subsystem

The VX7 video subsystem consists of a color TFT display. The video subsystem complies with the VESA VL bus standard. The resolution of this display is 800 by 600 pixels. This resolution complies with the SVGA graphics industry standard. The display can also be configured for 640 x 480 pixels.

The display supports screen blanking to eliminate driver distraction when the vehicle is in motion.

Power Supply

Vehicle power input for the VX7 is 12V to 80V DC nominal and is accepted without the need to perform any manual operation within the VX7.

If 12V to 60V DC power is not available – for example, in an office environment – an optional external Universal Input Power Supply can be used to convert AC wall power to an appropriate DC level.

Power input is fused for protection and the fuse is externally accessible.

Uninterruptible Power Supply

A DC uninterruptible power supply (UPS) battery is available to maintain power to the VX7 for a minimum of 15 minutes when vehicle power is not available (such as when a vehicle battery is being swapped).

Backup Battery

The VX7 has a permanent 190mAh Lithium battery installed to maintain time, date and CMOS setup information. The lithium battery is not user serviceable and should last five years with normal use before it requires replacement.

Note: The backup battery should only be changed by authorized service personnel.

Audio Interface

Speakers are located on the front on either side of the logo. An audio jack is available for headset operation. When a headset is plugged into the audio jack on the bottom of the VX7, the main speakers are disabled.

Card Slots

All card slots are located behind the User Access Panel.

Depending on the configuration ordered for the VX7, the following card slots may be present.

PCMCIA Slots

Microsoft Windows CE Plug and Play operating system controls the PCMCIA cards. These cards are hot swappable per the PCMCIA specifications.

CompactFlash (CF) Slot

If present, the CF ATA slot is not hot swappable. The VX7 must be powered down to insert or remove an ATA card. When the CF slot is present, the operating system is stored on the CF ATA card and the VX7 cannot operate without the ATA card.

Secure Digital (SD) Slot

If a CF ATA card slot is present, the SD slot accepts an SD memory card. In this case, the SD card is hot swappable.

If a CF ATA card slot is not present, the SD slot is not hot swappable. The operating system is stored on the SD card in this case and the VX7 cannot operate without this card.

Bluetooth LXEZ Pairing

The VX7 contains Bluetooth version 2.0 with Enhanced Data Rate (EDR) up to 3.0 Mbit/s over the air. Bluetooth device connection (or pairing) can occur at distances up to 32.8 ft (10 meters) Line of Sight. The wireless client retains wireless connectivity while Bluetooth is active.

The user will not be able to select PIN authentication or encryption on connections to from the VX7. However, the VX7 supports authentication requests from pairing devices. If a pairing device requests authentication or encryption, the VX7 displays a prompt for the PIN or passcode. Maximum encryption is 128 bit. Encryption is based on the length of the user's passcode.

Bluetooth filtered mode simultaneously supports one printer as a slave Bluetooth device and one scanner, either as a slave or as a master Bluetooth device.

- The VX7 does not have a Bluetooth managed LED.
- The LED on the Bluetooth scanner illuminates during a scanning operation.
- Barcode data captured by the Bluetooth scanner is manipulated by the settings in the VX7 Scanner Properties control panel applet.
- Multiple beeps may be heard during a barcode scan using a mobile Bluetooth scanner; beeps from the mobile Bluetooth scanner as the barcode data is accepted/rejected, and other beeps from the VX7 during final barcode data manipulation.

See also: Start > Settings > Bluetooth

Power Modes

The VX7 has four power modes: On, User Idle, Suspend and Off.

Note: The VX7 does not support System Idle mode.

On Mode

When the VX7 is attached to either vehicle 12-80 VDC or an external power supply and the power button is pressed, the VX7 is in the On mode. In this mode, the keypad, touch screen and any attached peripherals such as a scanner function normally. The display remains on until the backlight timer (if enabled) expires.

User Idle Mode

If the Display Backlight Timer is enabled (Start > Settings > Control Panel > Display), the VX7 enters User Idle Mode when the display backlight timer expires without any Primary Event (see below) to reset the timer. The VX7 exits User Idle Mode with any Primary Event.

The keypress or screen touch that exits User Idle Mode is sent to the operating system.

The VX7 then transitions to On Mode.

Primary Events

- Any key on the keypad
- COM1 activity
- Stylus touch on the touch screen
- Scanner activity
- Power button tap
- USB client connection
- Bluetooth device reconnect / disconnect message

Suspend Mode

The VX7 does not support Suspend mode. However, if the Suspend timer is enabled (**Start > Settings > Control Panel > Power**), the VX7 transitions to Off mode when the Suspend timer expires.

Off Mode

The VX7 turns off if the user presses the power button when the VX7 is On. The VX7 is also off when it is not connected to a power source. However, an internal Real Time Clock (RTC) powered by an internal battery maintains the date and time while the VX7 is off.

External Connectors

Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

Most external connectors for the VX7 are located on the bottom of the unit.

- The Keyboard/Mouse connector accepts a VMT keyboard or a dongle cable for a PS/2 keyboard and mouse.
- COM1 connects to a serial barcode scanner.
- COM3 (labeled “COM2/3”) connects to a serial printer or PC with the appropriate cables.
- The USB and optional Ethernet connector accepts dongle cables, offering a combination of the following ports:
    - An Ethernet port (optional)
    - A USB Host port
    - A USB Client port.
- Audio connects to a mono or stereo telephone headset/microphone.

Antenna connectors are located on the top of the VX7. VX7’s can be configured for a single antenna or dual antennas.

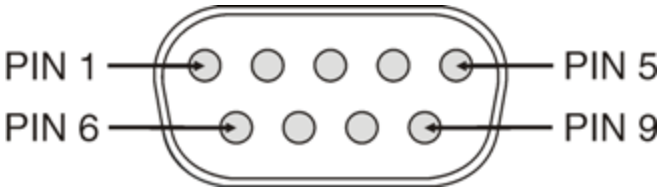
Scanner Serial Connector (COM1)

Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

The serial connector, labeled “SCANNER”, (configured as COM1) is industry-standard RS-232. The connector includes a PC/AT standard 9–pin “D” male connector.

By default, Pin 9 is configured to supply +5 VDC at 0.4A (max) for an external barcode scanner. Pin 9 may also be configured to provide RI.

If COM1 is not being used for a scanner, it can also be used for screen blanking when the vehicle is in motion.



Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	+5VDC or RI	Bar Code Scanner Power - 400mA max or Ring Indicator - Input
Shell	CGND	Chassis Ground

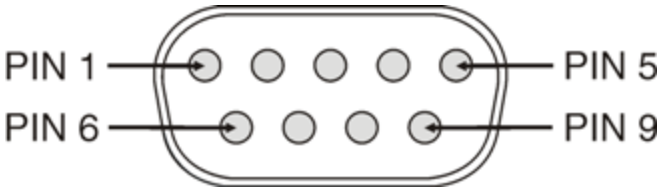
Printer / PC Serial Connector (COM3)

Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

The serial connector, labeled “COM2/3”, is industry-standard RS-232. The connector includes a PC/AT standard 9–pin “D” male connector.

By default, Pin 9 provides RI. Pin 9 may also be configured to supply +5 VDC at 0.4A (max) for an external bar code scanner.

If COM3 is not being used for a scanner, it can also be used for screen blanking when the vehicle is in motion.

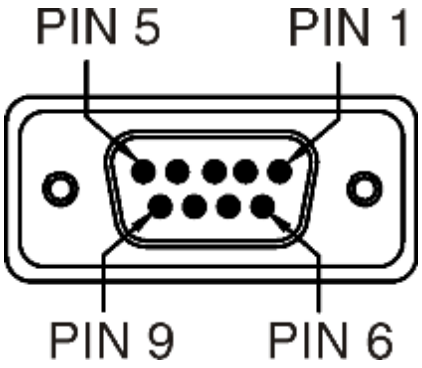


Pin	Signal	Description
1	DCD	Data Carrier Detect – Input
2	RXD	Receive Data – Input
3	TXD	Transmit Data – Output
4	DTR	Data Terminal Ready – Output
5	GND	Signal/Power Ground
6	DSR	Data Set Ready – Input
7	RTS	Request to Send – Output
8	CTS	Clear to Send – Input
9	RI or +5VDC	Ring Indicator – Input (default) or Bar Code Scanner Power – 400mA max
Shell	CGND	Chassis Ground

Technical Specifications - Connection Cable

The exact serial cable is crucial. Many commercial null modem cables will not work. The following cable is recommended:

Serial Cable - 9000060CABLE



DB9 female	DB9 female
1	7
2	3
3	2
4	6, 8
5	5
6, 8	4
7	1
9	No Connection

Some laptop devices do not properly implement all control lines on the serial port - the laptop connection will not work.

RTS/CTS Handshaking and the Serial Port

RTS Ready to Send

CTS Clear to Send

DTR Data Terminal Ready

DSR Data Set Ready

Remote Side The device sending data to and receiving data from the VX7 through the serial cable connected to the RS-232 ports on both devices.

Serial Cable: 9000060CABLE

The VX7 serial port supports four types of handshaking via the serial cable: None, standard Xon/Xoff, standard DTR/DSR, and a form of RTS/CTS.

To use RTS/CTS, the remote side computer must clear the DTR line which sets the VX7 CTS line and allows the VX7 to send data to the remote side.

And then signals and data travel smoothly between both devices.

Screen Blanking Cable

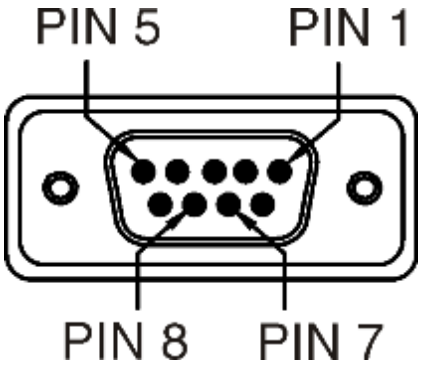
The customer must supply their own cable.

The cable must be designed so that pin 7 (RTS – Request to Send Output) and pin 8 (Clear to Send Input) of a D9 female connector provide continuity only when the vehicle is stopped (for example, via a switch on the accelerator pedal of the fork truck).

All other pins on the connector must be left unconnected. If pins 7 and 8 do not provide continuity (or the cable is removed), the VX7 screen remains blank.

Serial Cable

Customer built cable with the following specifications.



DB9 female	Function
1	Not Used
2	Not Used
3	Not Used
4	Not Used
5	Not Used
6	Not Used
7	No signal when in motion, Continuity to Pin 8 when stopped
8	No signal when in motion, Continuity to Pin 7 when stopped
9	Not Used

Sample Cable for Screen Blanking

Proper COM port settings to support screen blanking are located in Start > Settings > Control Panel > Scanner.

PS/2 Keyboard/Mouse

A standard PS/2 keyboard and mouse can be attached to the VX7 using the appropriate dongle cable.

The dongle cable attaches to the VX7 and provides two PS/2 connectors, one labeled “Keyboard” and one labeled “Mouse”. Please refer to documentation provided with the PS/2 keyboard and mouse for more information on their operation.

USB Keyboard / Mouse

A standard USB mouse can be attached to the VX7 using the appropriate dongle cable.

A standard USB keyboard can be attached to VX7’s using the appropriate dongle cable.

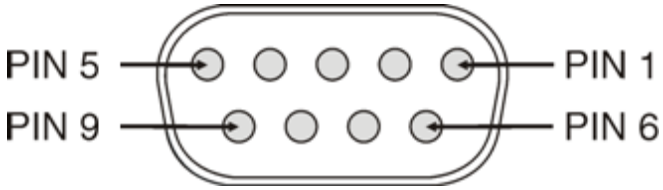
The dongle cable attaches to the VX7 and provides a USB connector. Please refer to documentation provided with the USB keyboard and mouse for more information on their operation.

Keyboard / Mouse Connector

Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

The external keyboard connector accepts:

- A VMT keyboard with integrated pointing device
- A VMT keyboard without integrated pointing device
- A dongle cable providing PS/2 connections for a standard PS/2 keyboard and mouse.



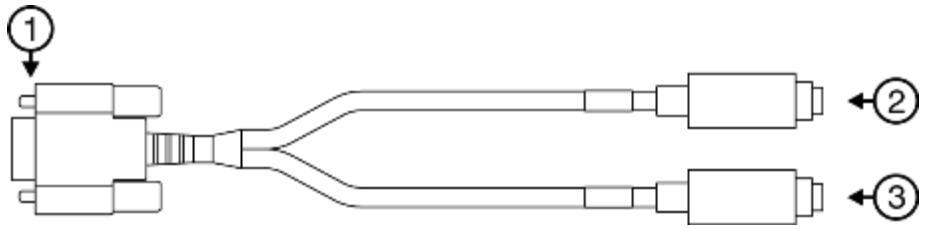
The +5V supply available from the connector is current limited at 400mA.

Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	MSDAT_A	Mouse Data
3	-	Not Connected
4	MSCLK_A	Mouse Clock
5	DGND	System Ground
6	-	Not Connected
7	KBCLK_A	Keyboard Clock
8	BL_ENABLE	Keyboard Backlight Enable
9	KDB_PWR	Keyboard Power, 5V, 400mA max.
Shell	CGND	Chassis Ground

PS/2 Keyboard / Mouse Cable

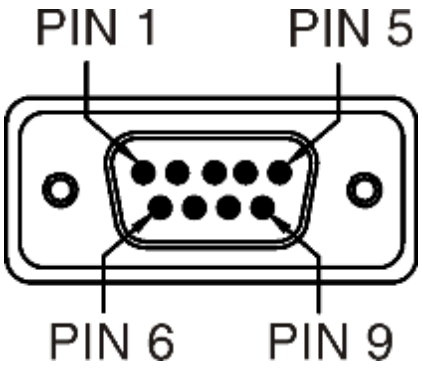
Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

The PS/2 keyboard/mouse dongle cable allows a standard PS/2 keyboard and/or mouse to be attached to the VX7. The PS/2 connectors on the dongle cable are labeled for keyboard and mouse.



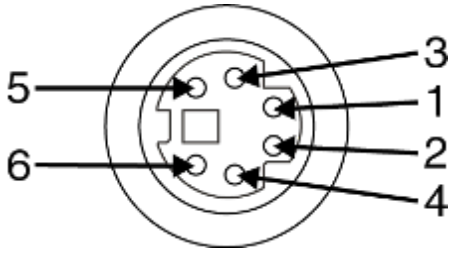
1. D9 Connector
2. PS/2 Keyboard Connector
3. PS/2 Mouse Connector

D9 Male Connector



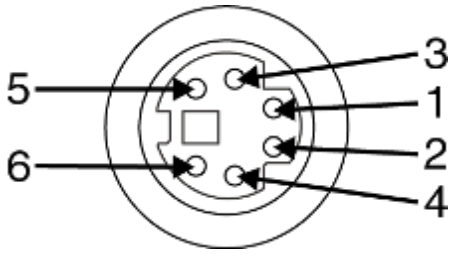
Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	MSDAT_A	Mouse Data
3	-	Not Connected
4	MSCLK_A	Mouse Clock
5	DGND	System Ground
6	-	Not Connected
7	KBCLK_A	Keyboard Clock
8	BL_ENABLE	Keyboard Backlight Enable
9	KDB_PWR	Keyboard Power, 5V, 400mA max.
Shell	CGND	Chassis Ground

PS/2 Keyboard Connector



Pin	Signal	Description
1	KBDAT_A	Keyboard Data
2	--	Not Connected
3	DGND	System Ground
4	KBD_PWR	Keyboard Power, 5V
5	KBCLK_A	Keyboard Clock
6	--	Not Connected
Shell	CGND	Chassis Ground

PS/2 Mouse Connector



Pin	Signal	Description
1	MSDAT_A	Mouse Data
2	--	Not Connected
3	DGND	System Ground
4	KBD_PWR	Keyboard Power, 5V
5	MSCLK_A	Mouse Clock
6	--	Not Connected
Shell	CGND	Chassis Ground

USB and Optional Ethernet Connector

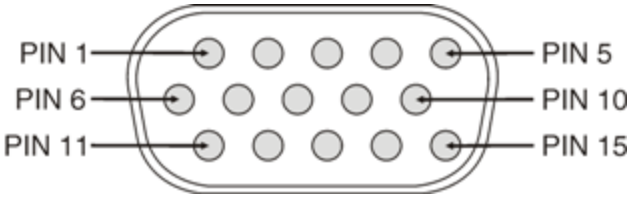
Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

After the cable is attached to the VX7, USB devices can be hot swapped.

The VX7 Ethernet/USB connector accepts dongle cables that provide combinations of the following connections:

- an Ethernet port, via an RJ45 connector (optional)
- a USB Host port for connecting a USB device to the VX7
- a USB Client port to connect the VX7 to a USB host or hub.

Note: Ethernet is optional on the VX7. If the VX7 was not ordered with Ethernet, the Ethernet connection on the dongle cable has no function.

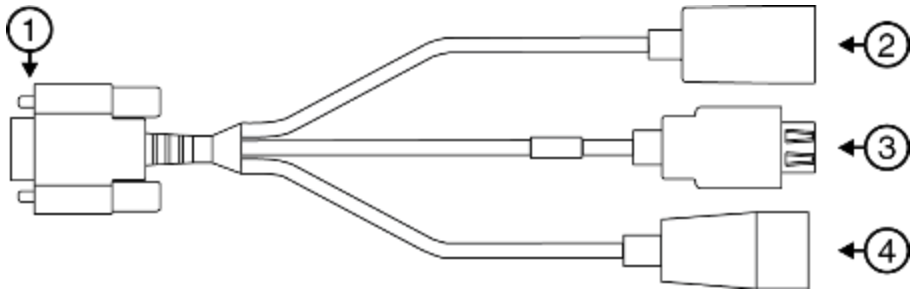


Pin	Signal	Description
1	USB2N_A	USB D-
2	-	Not Connected
3	-	Not Connected
4	RXP	Receive +
5	RXN	Receive -
6	USB2P_A	USB D+
7	DGND	USB Power Return
8	-	Not Connected
9	RJ45_45	RJ45, Pins 4 and 5
10	RJ45_78	RJ48, Pins 7 and 8
11	5V_USB_23	USB Power, current limited
12	-	Not Connected
13	-	Not Connected
14	TXN	Transmit -
15	TXP	Transmit +
Shell	CGND	Chassis Ground

Ethernet / USB Dongle Cables

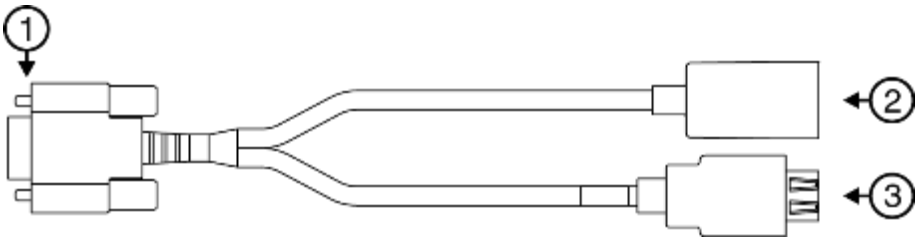
Power the VX7 off before attaching a cable to any port (serial, keyboard, Ethernet/USB, etc.).

Ethernet support is optional on the VX7



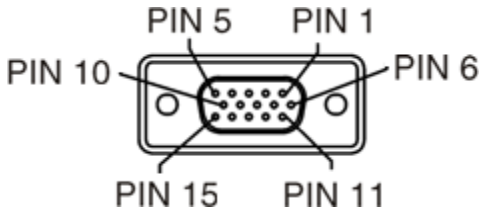
1. D15 Connector
2. RJ45 Connector
3. USB Host Connector
4. USB Client Connector

The 9000075CABLE above is required when using ActiveSync via USB on the VX7.



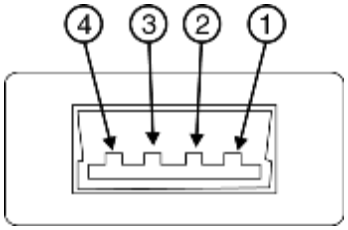
1. D15 Connector
2. RJ45 Connector
3. USB Host Connector

D15 Female Connector



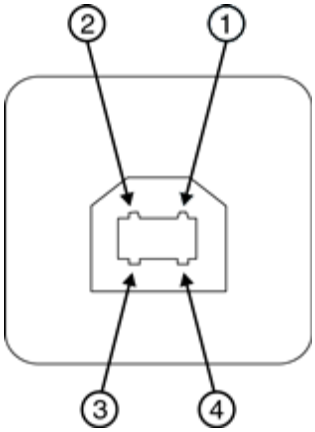
Pin	Signal	Description
1	USB2N_A	USB D-
2	-	Not Connected
3	-	Not Connected
4	RXP	Receive +
5	RXN	Receive -
6	USB2P_A	USB D+
7	DGND	USB Power Return
8	-	Not Connected
9	RJ45_45	RJ45, Pins 4 and 5
10	RJ45_78	RJ48, Pins 7 and 8
11	5V_USB_23	USB Power, current limited
12	-	Not Connected
13	-	Not Connected
14	TXN	Transmit -
15	TXP	Transmit +
Shell	CGND	Chassis Ground

USB Host Connector



Pin	Signal	Description
1	5V_USB_23	USB Power, current limited
2	USB2N_A	USB D-
3	USB2P_A	USB D+
4	DGND	USB Power Return
Shell	CGND	Chassis Ground

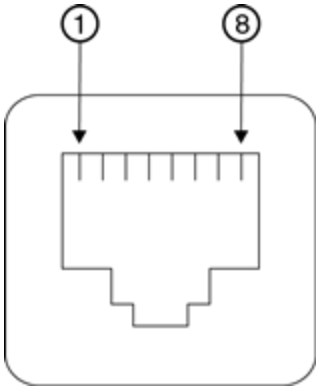
USB Client Connector



Pin	Signal	Description
1	5V_USB_23	USB Power, current limited
2	USB2N_A	USB D-
3	USB2P_A	USB D+
4	DGND	USB Power Return
Shell	CGND	Chassis Ground

RJ45 Connector

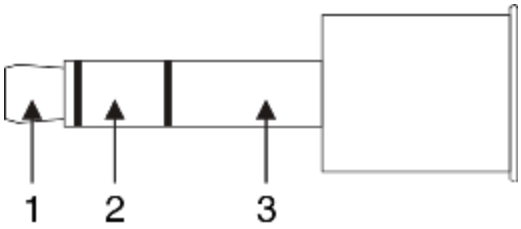
Note: This port is functional only when the VX7 is ordered with Ethernet.



Pin	Signal	Description
1	TXP	Transmit +
2	TXN	Transmit -
3	RXP	Receive +
4	-	Not Connected
5	-	Not Connected
6	RXN	Receive -
7	-	Not Connected
8	-	Not Connected

Audio Connector

The VX7 audio connector accepts a headset with a 2.5mm plug, such as a mono telephone headset with microphone or a stereo headset.



1. Microphone
2. Speaker
3. Ground

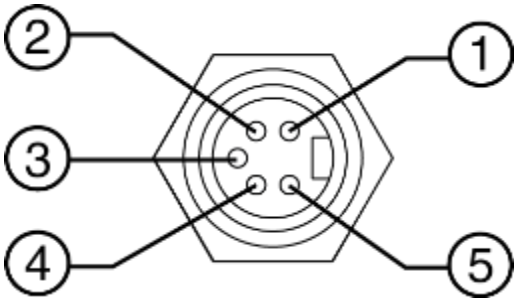
Please refer to **Start > Settings > Control Panel > Mixer** for information on configuring the audio port for either a mono headset with microphone or a stereo headset.

Note: The VX7 is not configured for standard PC speakers.

Power Supply Connector

Power is supplied to the VX7 through the power connector. Additionally this assembly provides a connection point for the vehicle's chassis ground to be connected internally to the conductive chassis of the computer.

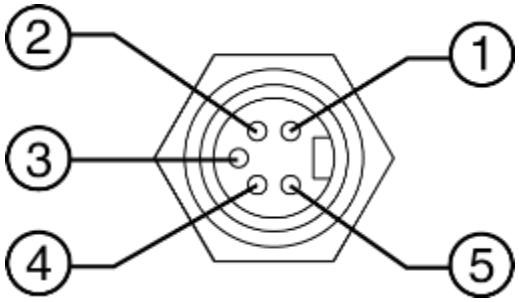
The VX7 internal power supply can accept DC input voltages in the range of 12 to 80 Volts DC.



1. DC Positive (+)
2. UPS Battery Positive (+)
3. Chassis Ground
4. UPS Battery Negative (-)
5. DC Negative (-)

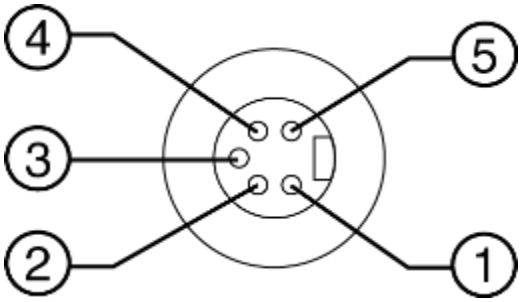
UPS Battery Pack Connectors

Input Connector Pinout



1. DC Positive (+)
2. Not Used
3. Chassis Ground
4. Not Used
5. DC Negative (-)

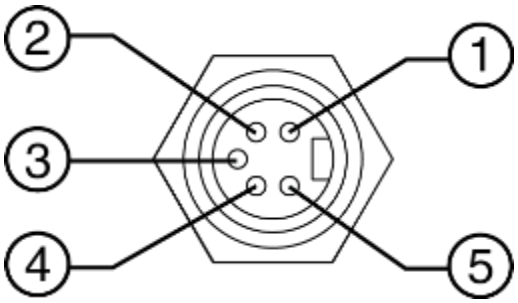
Output Connector Pinout



1. DC Positive (+)
2. UPS Battery Positive (+)
3. Chassis Ground
4. UPS Battery Negative (-)
5. DC Negative (-)

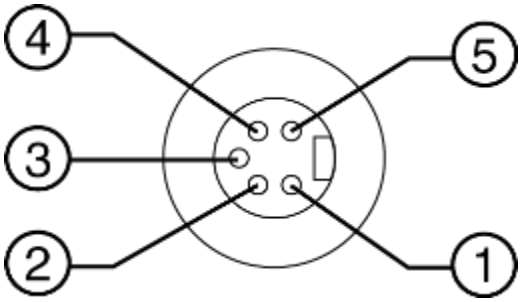
UPS Battery Extension Cable Connector

Input Connector Pinout



1. DC Positive (+)
2. UPS Battery Positive (+)
3. Chassis Ground
4. UPS Battery Negative (-)
5. DC Negative (-)

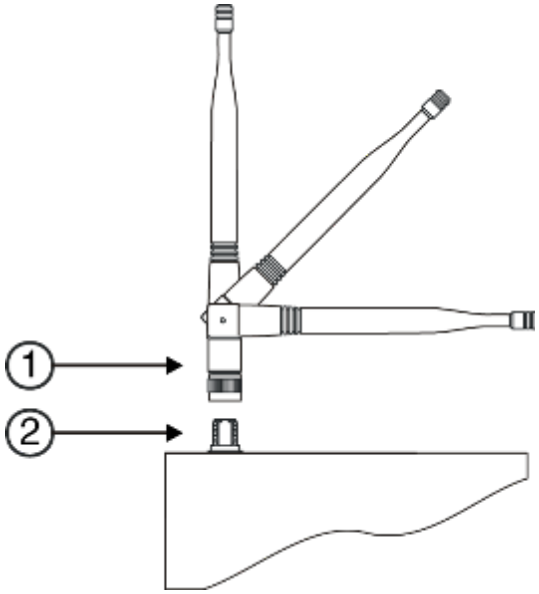
Output Connector Pinout



1. DC Positive (+)
2. UPS Battery Positive (+)
3. Chassis Ground
4. UPS Battery Negative (-)
5. DC Negative (-)

Antenna Connections

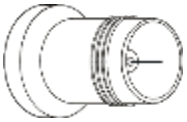
VX7's are equipped with a radio and require an either an external or an internal antenna. Some VX7's may be equipped with a dual antenna option. For these VX7's, an external antenna must be connected to each antenna connector.



1. Antenna
2. Antenna Connector

Spread Spectrum RF Antenna Connector Pin

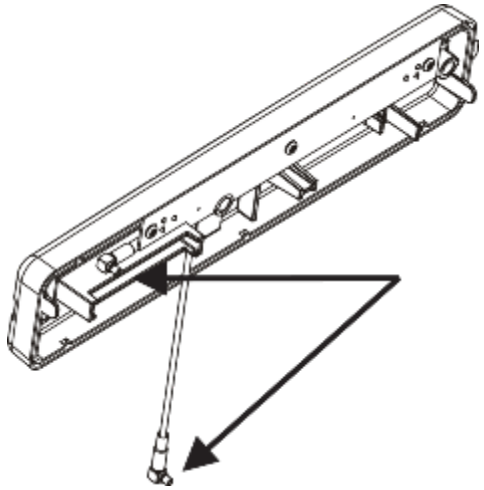
VX7's ordered with an external antenna option have either one or two antenna connectors located on top of the unit. VX7's ordered with the internal antenna option do not have an external antenna connector.



Vehicle Remote Antenna Mount

The external antenna (or antennas) can be remotely mounted on the vehicle. See VX7 Vehicle Mounting Reference Guide for instruction.

Internal Antenna

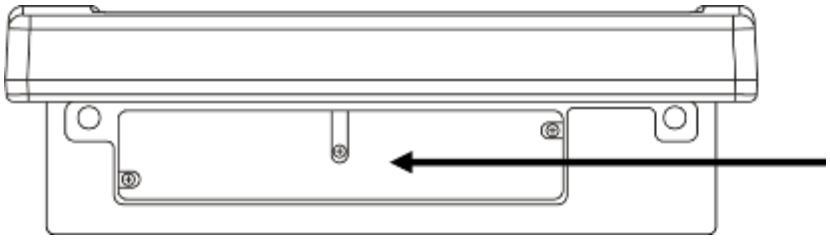


If the internal antenna option is ordered, an antenna is mounted on the inside of the user access panel cover. The internal antenna assembly has two antenna cables which are attached to the radio card.

User Access Panel

The User Access Panel cover can be removed to access the storage slots available on the VX7. The available slots and any factory installed cards in those slots depend upon the system configuration ordered.

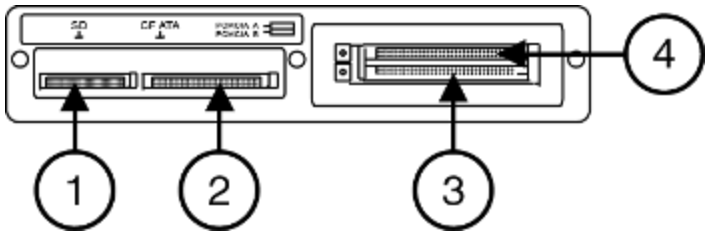
Remove User Access Panel Cover



1. Turn the VX7 off and detach the power cable.
2. Loosen the three (3) Phillips head screws securing the access panel cover so the cover can be removed. The screws are a captive part of the cover and cannot be removed.
3. Move the tethered cover aside to access the card slots. Use care not to unplug or damage the antenna leads. If the VX7 has an internal antenna, it is secured to the inside of the cover.

⚠	Although some cards can be hot swapped, the VX7 is not environmentally sealed while the access panel cover is removed to hot swap cards. Honeywell recommends powering off the VX7 and disconnecting the power cable before removing the user access panel.

Inside the User Access Panel



1. SD Card Slot
2. CF Card Slot (if present)
3. PCMCIA Slot B
4. PCMCIA Slot A

- If a CF card slot is present, the CF card contains the system files. The CF card must be present to boot the VX7.
- If a CF card slot is not present, the SD card contains the system files. The SD card must be present to boot the VX7.
- The 802.11 radio card is installed by the factory in PCMCIA Slot A. This card must remain in this slot to avoid damage to the antenna cables.

User provided storage cards can be installed in:

- SD card slot only if a CF card slot is present
- PCMCIA slot B, accepts Type I or II PCMCIA cards

Install or remove storage cards as desired.

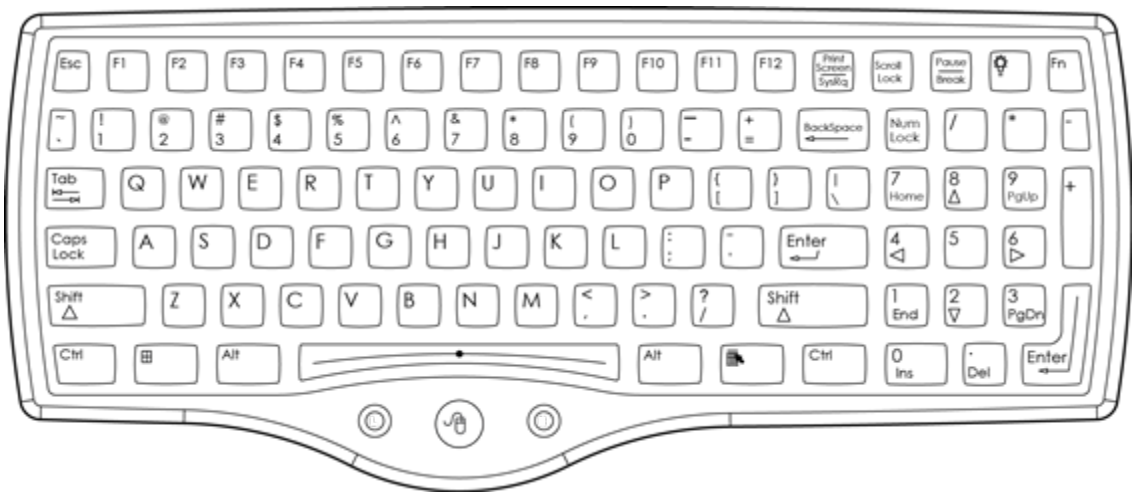
Reinstall User Access Panel Cover

1. Align the user access panel cover. Use care not to pinch the antenna leads, if present.
2. With a user supplied torque wrench and Phillips size 1 driver bit, tighten the screws to 9 inch pounds each.
3. Reconnect power and turn the VX7 on.
4. The Windows CE operating system automatically recognizes any storage cards that have been added or removed. Use the Windows explorer or My Computer to locate installed storage cards.

QWERTY 95 Key Keyboard

The VX7 has a QWERTY 95 key keyboard, designed for ease of use with the Windows CE operating system, the keyboard with pointing device connects via a cable to the keyboard port on the VX7. Additional Windows keys (the Windows logo key and the Application key) and an integrated pointing device are provided.

- The 95 key keyboard supports all 104 keyboard functions (101 standard keyboard plus Windows keys) and includes an integrated pointing device and left and right mouse buttons. However, because the keyboard only has 95 keys, all functions are not visible (or printed on the keyboard). Therefore the keyboard supports what is called **hidden keys** -- keys that are accessible but not visible on the keyboard.
- A key or combination of keys can be remapped to provide a single keypress, a string of keypresses or to execute an application or command. All key **remapping** is done using the KeyPad option in the Control Panel (**Start > Settings > Control Panel > Keypad**).
- The 95-key keyboard does not have a **2nd key function**.
- The 95 key keyboard does not have a **NumLock** indicator or key. NumLock is always On.
- The 95 key keyboard keys are backlit. The **keyboard backlight** and the display share the same timer, which is configured in **Start > Settings > Control Panel > Power**. When the display is On, the keyboard backlight is also On.



Keyboard Indicators

Numlock

For the 95-key keyboard, the NumLock key and the numeric keys are backlit green when NumLock is off.

When NumLock is on, the backlight for the NumLock key and the numeric keys is amber.

For information on preserving NumLock configuration after a reboot, please see **Start > Settings > Control Panel > MX3X-VXC Options > Misc** tab.

CapsLock

Default value for CapsLock is Off. For the 95-key keyboard, the CapsLock key is backlit green when CapsLock is off.

When CapsLock is on, the backlight for the CapsLock key is amber.

For information on preserving CapsLock configuration after a reboot, please see **Start > Settings > Control Panel > MX3X-VXC Options > Misc** tab.

Scroll Lock

Default value for Scroll Lock is Off. The Scroll Lock key is backlit green when Scroll Lock is off.

When Scroll Lock is on, the backlight for the Scroll Lock key is amber.

Keyboard Backlight

The keyboard backlight key in the top right hand corner has a light bulb icon.

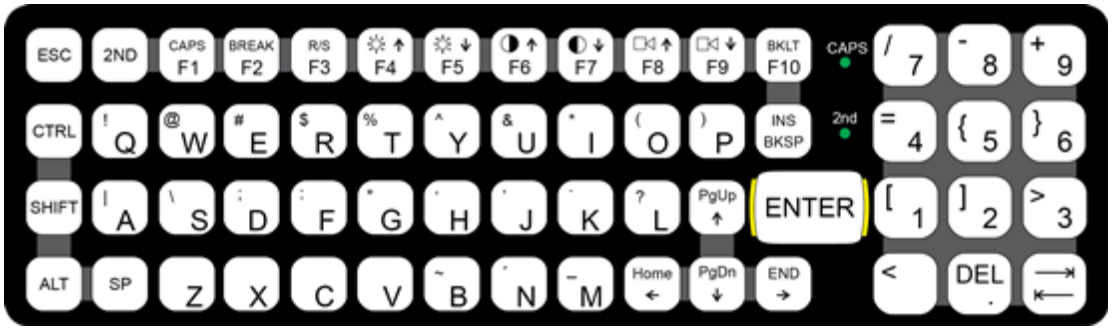
The keyboard keys are backlit. By default, the keyboard backlight and the display share the same timer, which is configured in **Start > Settings > Control Panel > Power**. When the display is On, the keyboard backlight is also On.

The keyboard backlight can also be manually controlled using the backlight key in the upper right hand corner of the keyboard. Pressing the backlight key cycles the keyboard backlight through the levels of backlight intensity: Off, Maximum intensity, Medium intensity, Low intensity.

QWERTY Keyboard

The VX7 has an optional 60 key QWERTY keyboard, available with a standard overlay, an IBM 3270 overlay or an IBM 5250 overlay. These keyboards have 101 keyboard functions, including a numeric keypad.

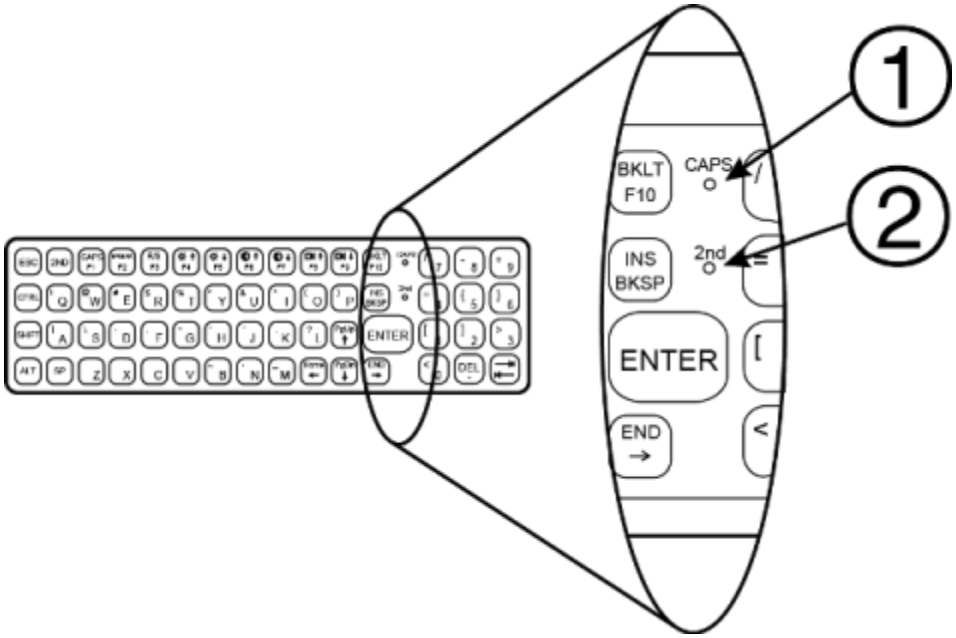
- The keyboard supports all 101 keyboard functions. However, because the keyboard only has 60 keys, all functions are not visible (or printed on the keyboard). Therefore the VX7 keyboard supports what is called **hidden keys** -- keys that are accessible but not visible on the keyboard.
- A key or combination of keys can be remapped to provide a single keypress, a string of keypresses or to execute an application or command. All key **remapping** is done using the KeyPad option in the Control Panel (**Start > Settings > Control Panel > Keypad**).
- The keyboard does not have a **NumLock** indicator or key. NumLock is always On.
- The keyboard keys are backlit. The **keyboard backlight** and the display share the same timer, which is configured in **Start > Settings > Control Panel > Power**. When the display is On, the keyboard backlight is also On.



IBM 3270 Overlay

IBM 5250 Overlay

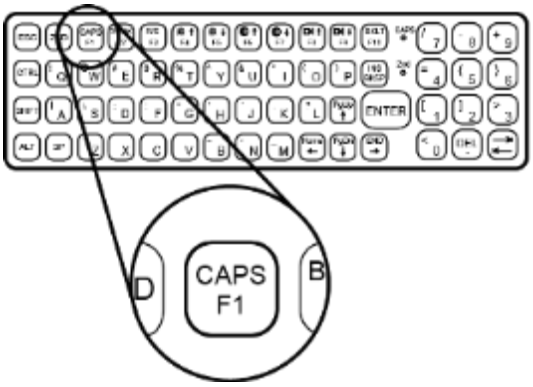
Keyboard LEDs



1. CapsLock Mode LED
2. Secondary Mode LED

CAPS LED

The CAPS LED indicates the state of the keyboard CapsLock mode. If CapsLock is enabled this LED is illuminated green. When CapsLock is off, the LED is dark.

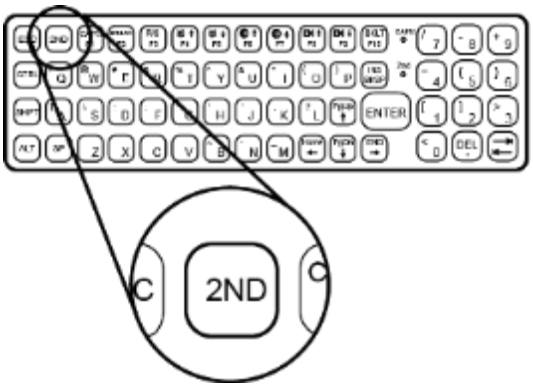


Press <2nd> then <F1> to toggle CapsLock On and Off. The default value of CapsLock is “Off”. For information on preserving CapsLock configuration after a reboot, please see **Start > Settings > Control Panel > MX3X-VXC Options > Misc** tab.

Secondary Keys LED

The VX7 keyboard is equipped with several secondary keys. These keys are identified by the superscripted text found on the keyboard keys.

The secondary keys are accessible by using two (2) keystrokes: the <2nd> key followed by the superscripted key.



Once the <2nd> state is enabled (by pressing the <2nd> key) the Secondary Mode LED is illuminated and the <2nd> state is enabled until another key is pressed.

The <2nd> key is toggled on with a <2nd> keypress and then immediately off with another <2nd> keypress.

For example:

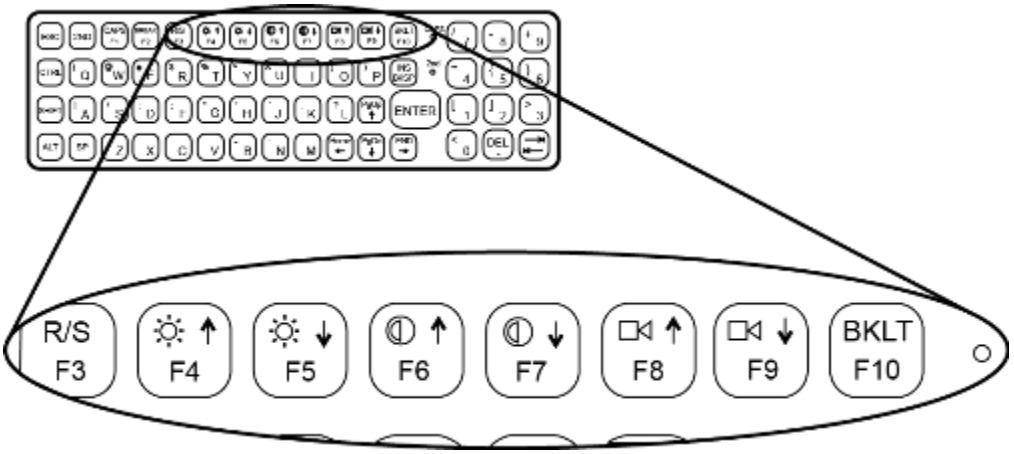
Press <2nd> and <F1> to turn CapsLock on and off.

Press <2nd> and <↑> to initiate the PgUp command.

Press <2nd> and <Q> to type the “!” key.

Press <2nd> and <BkSp> to enter the Insert (Ins) mode.

Control Keys



The VX7 keyboard has several control keys, some of which are not used:

- The 2nd function of the **<F3>** key is not used as Windows Power Management controls all power management modes on the VX7.
- The 2nd functions of the **<F4> and <F5>** keys are not used as the display brightness is adjusted via the buttons on the control panel.
- The 2nd functions of the **<F6>, and <F7>** keys are not used as the VX7 has TFT LCD screen with no provision for contrast adjustments.
- The 2nd functions of the **<F8> and <F9>** keys are not used as the sound volume on the VX7 is controlled with the Volume and Sounds icon in the Microsoft Windows CE Control Panel.
- The 2nd function of the <F10> key is not used as the display backlight timer also controls the keyboard backlight.

LED Functions

Note: The VX7 does not have a Bluetooth managed LED.

Status LED

The Status LED is located above the power (on/off) switch.

- Green – VX7 is operating from vehicle power or AC power.
- Solid Yellow – VX7 is operating from the UPS, UPS battery is good.
- Flashing Yellow – VX7 is operating from the UPS, UPS battery is critically low.

60 Key Keyboard - Keyboard LEDs

The keyboard LEDs turn on for about one second when the operating system loads the keyboard driver.

- On an external USB keyboard, the NumLock, CapsLock and Scroll Lock keys blink the same as a desktop PC. If the LEDs blink more than once, this indicates a keyboard problem.
- On the 60-key keyboard, only the CAPs LED is lit during this process. If the LEDs blink more than once, this indicates a keyboard problem.

On the 60-key keyboard, the **2nd LED** is lit when the 2nd key has been pressed. It remains illuminated until the 2nd key is pressed again, or a second-function key has been pressed.

On the 60-key keyboard, the **CAPS LED** is lit when the CAPS/F1 key has been pressed. It remains illuminated until the CAPS/F1 key is pressed again.

Speakers

There are two speakers located at the top of the VX7, one on either side of the logo.

The speakers have a loudness of at least 95 dBm at 10 cm measured in front of the unit. Speaker volume is adjustable via the Control Panel or by an application through the use of an API call. The minimum volume level is 0 (no sound) with a default setting of maximum non-distorted volume. The volume sticks at maximum and minimum levels.

Speaker volume is enabled and adjusted using the Volume & Sounds control panel (**Start > Settings > Control Panel > Volume and Sounds**).

Operational “beeps” are emitted from the speaker.

Display

The display is a thin-film transistor display capable of supporting half screen SVGA+ graphics modes. Display size is 800 x 600 pixels. The display covering is designed to resist stains. The touch screen allows signature capture and touch input. The display supports screen blanking to eliminate driver distraction when the vehicle is in motion.

Touch Screen

The touch screen is a Resistive Panel with a scratch resistant finish that can detect touches by a stylus, and translate them into computer commands. In effect, it simulates a computer mouse. Only Delrin or plastic styluses should be used. A right mouse click is simulated by touching and holding the screen for the appropriate time interval.

Always use the point of the stylus for tapping or making strokes on the display. Never use an actual pen, pencil, sharp or abrasive object to write on the touch screen.

An extra or replacement stylus may be ordered.

A replaceable touch screen protective film is available for when the VX7 is used in an abrasive environment. Contact Technical Assistance for availability.

Touch Screen Heater

Extended temperature versions of the VX7 contain a touch screen heater. The touch screen heater can be disabled when not needed (**Start > Settings > Control Panel > MX3-VXC Options**).

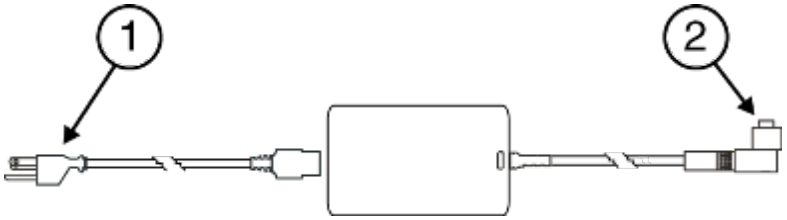
Power Supply

AC to DC power input for the VX7 is delivered via an optional external power supply and adapter cable.

Vehicle power input for the VX7 is 12V to 80V DC nominal and is accepted without the need to perform any manual operation within the VX7.

An optional uninterruptible power supply (UPS) battery can be used with the vehicle DC power supply. Power input is fused for protection and the fuse is externally accessible on the VX7.

External Power Supply



1. AC Input Cable (US Only)
2. DC Output Cable

In North America, this unit is intended for use with a UL Listed ITE power supply with output rated 12 – 80 VDC, minimum 15 W. Outside North America, this unit is intended for use with an IEC certified ITE power supply with output rated 12 – 80 VDC, minimum 15 W.

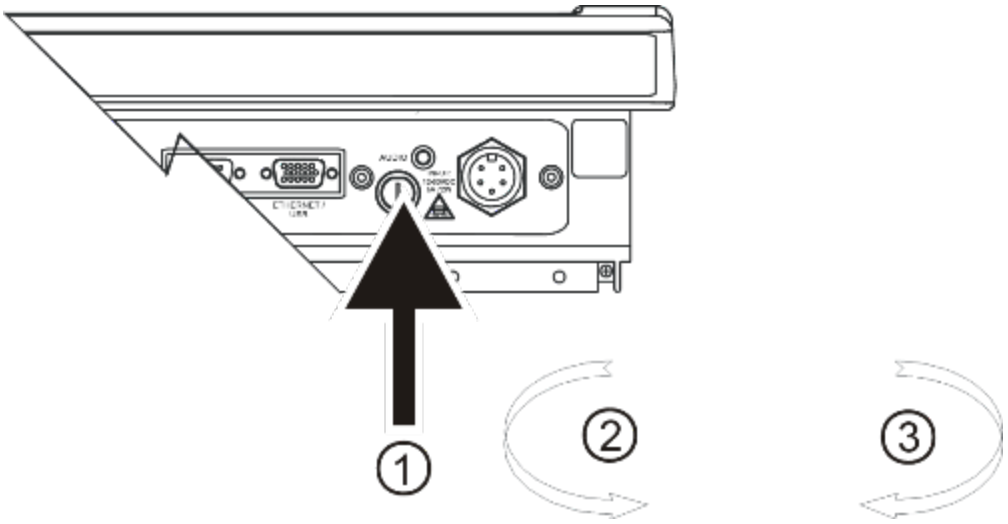
The external power supply may be connected to either a 120V, 60Hz supply or, outside North America, to a 230V, 50Hz supply, using the appropriate detachable cordset. In all cases, connect the external AC supply to a properly grounded source of supply provided with maximum 15 Amp overcurrent protection (10 Amp for 230V circuits).

Fuse

The VX7 uses a 100V, 10A time delay (slow blow), high current interrupting rating fuse that is externally accessible and user replaceable.

Should it need replacement, replace with same size, rating and type of fuse – Littlefuse 0234010 or Optifuse MSC-10A (5x20mm).

Fuse has voltage on it even when power is off. Always disconnect input power before changing the fuse.



Fuse Replacement

1. Fuse
2. Twist in this direction to remove
3. Twist in this direction to insert

Chapter 3: Software

Introduction

There are several different aspects to the setup, configuration and operation of the VX7. Many of the setup and configuration settings are dependent upon the optional features such as hardware and software installed on the unit. The examples found in this section are to be used as examples only, the configuration of your specific VX7 computer may vary. The following sections provide a general reference for the configuration of the VX7 and some of its optional features.

Operating System

Your VX7 operating system is Microsoft® Windows® CE 5. The VX7 operating system revision is displayed on the Desktop. This is the default setting for the Desktop Display Background.

Windows CE Operating System

Note: For general use instruction, please refer to commercially available Windows CE user's guides or the Windows CE on-line Help application installed with the VX7

This segment assumes the system administrator is familiar with Microsoft Windows options and capabilities loaded on most standard Windows computers.

Therefore, the sections that follow describe only those Windows capabilities that are unique to the VX7 and its Windows CE environment.

General Windows CE Keyboard Shortcuts

Use the keyboard shortcuts in the chart below to navigate with the VX7 keyboard. These are standard keyboard shortcuts for Windows CE applications.

Press these keys …	To …
CTRL + C	Copy
CTRL + X	Cut
CTRL + V	Paste
CTRL + Z	Undo
DELETE	Delete
SHIFT with any of the arrow keys	Select more than one item in a window or on the desktop, or select text within a document.
CTRL+A	Select all.
ALT+ESC	Cycle through items in the order they were opened.
CTRL+ESC	Display the Start menu.
ALT+Underlined letter in a menu name	Display the corresponding menu.
Underlined letter in a command name on an open menu	Carry out the corresponding command.
ESC	Cancel the current task.

The touch screen provides equivalent functionality to a mouse:

- A touch on the touch screen is equivalent to a left mouse click.
- Many items can be moved by the “drag and drop” method, touching the desired item, moving the stylus across the screen and releasing the stylus in the desired location.
- A double stylus tap is equivalent to a double click.
- A touch and hold is equivalent to a right mouse click[1].
- *Devices with Shift and Ctrl Keys* The Shift and Ctrl keys can be used with the touch screen for multiple selection of items.
    - To select disconnected items, press the Ctrl key and then touch each item to be selected in the set. Press the Ctrl key again to terminate this mode.
    - To select a connected set of items, press the Shift key, then touch the first item in the series. Touch the last item in the series. Press the Shift key again to terminate the selection mode.

[1] Some applications may not support this right click method. Please review documentation for the application to see if it provides for right mouse click configuration.

Warmboot

A warmboot reboots the computer without erasing any registry data. However, any applications installed to RAM are lost, as is all data in RAM. This occurs because the operating system is stored on the flash drive, but must be loaded into RAM to run.

All registry configurations are automatically preserved. Any applications stored as .CAB files in the System folder and configured in the Registry to persist are reinstalled on boot up by the Launch utility.

Coldboot

A coldboot reboots the computer, erases all registry data and returns the computer to factory default settings. In order to be preserved, applications and data must be stored in the System folder. Registry information is not preserved. Only factory default applications and drivers stored as .CAB files in the System folder are loaded by Launch.

A cold boot is initiated by running the Coldboot application in the Windows folder. This application automatically cold boots the VX7, erasing any customer applied registry changes and returning the VX7 to its factory settings.

Clearing Persistent Storage / Reset to Default Settings

The coldboot utility sets all registry settings back to factory defaults. No other clearing is available or necessary.

Folders Copied at Startup

If any of the following folders are created in the System folder, they are copied at startup:

System\Desktop	copied to	Windows\Desktop
System\Favorites	copied to	Windows\Favorites
System\Fonts	copied to	Windows\Fonts
System\Help	copied to	Windows\Help
System\Programs	copied to	Windows\Programs
AppMgr	copied to	Windows\AppMgr
Recent	copied to	Windows\Recent

This function copies only the folder contents, no sub-folders.

The Windows\Startup folder is not copied on startup because copying this folder has no effect on the system or an incorrect effect.

Files in the Startup folder are executed, but only from System\Startup. Windows\Startup is parsed too early in the boot process so it has no effect.

Executables in System\Startup must be the actual executable, not a shortcut, because shortcuts are not parsed by Launch.

Saving Changes to the Registry

The VX7 saves the registry when you:

- Tap **Start > Run** then type **Warmboot**. Tap **OK**.

The registry save process takes 0 – 3 seconds. If nothing has been changed, nothing is saved (e.g. 0 seconds).

The registry is automatically saved every 20 minutes. It is also saved every tenth time the registry settings are changed. Registry settings are changed when control panel applet (e.g. Date/Time) parameters are changed by the user and a warm boot was not performed afterward.

When you tap **Start > Run** then type Coldboot and tap the OK button, factory default registry settings are loaded during coldboot. All customized changes and settings are lost.

Software Load

The software loaded on the VX7 consists of Microsoft® Windows® CE 5 OS, hardware-specific OEM Adaptation Layer, device drivers, Internet Explorer 6.0 for Windows CE browser and utilities. The software supported is summarized below:

- Full Operating System License: Includes all operating system components, including Microsoft® Windows® CE 5 kernel, file system, communications, connectivity (for remote APIs), device drivers, events and messaging, graphics, keyboard and touch screen input, window management, and common controls.
- Network and Device Drivers
- Bluetooth (Optional)

Note: Please contact your Honeywell representative for software updates and CAB files as they are released by Honeywell.

Software Applications

The following applications are included:

- WordPad
- Scan Wedge (barcode result manipulation)
- ActiveSync
- Transcriber
- Internet Explorer
- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer

Note that the viewer applications allow viewing documents, but not editing them.

ActiveSync

ActiveSync is pre-loaded on all VX7 devices. Using Microsoft ActiveSync you can copy files from your VX7 to your desktop/laptop , and vice versa. After an ActiveSync relationship (partnership) has been established with a desktop/laptop, ActiveSync will automatically startup each time the VX7 is cabled to the desktop/laptop.

Bluetooth (Optional)

Start > Settings > Control Panel > Bluetooth

Only installed on a Bluetooth equipped VX7. The System Administrator can Discover and Pair targeted Bluetooth devices for each VX7. The System Administrator can enable / disable Bluetooth settings and assign a Computer Friendly name for each VX7.

The Bluetooth control panel can also be accessed by doubletapping the Bluetooth icon in the taskbar or on the desktop.

Java (Optional)

Files can be accessed by tapping **Start > Programs > JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. Honeywell does not support Java applications running on

the mobile device.

RFTerm (Optional)

Start > Programs > RFTerm

The application can also be accessed by double clicking the RFTerm desktop icon.

Avalanche

The Wavelink Avalanche Enabler installation file is loaded on the VX7; however, the device is not configured to launch the installation file automatically. The installation application must be run manually the first time Avalanche is used. Following installation, the Wavelink Avalanche Enabler will be an auto-launch application. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

Software Development

See Also: CE API Programming Guide

The CE API Programming Guide documents device-specific API calls for the VX7. It is intended as an addition to Microsoft Windows CE API documentation.

A Software Developers Kit (SDK) and additional information about software development can be found on the Developer Portal. Contact Technical Assistance for more information or to access the portal.

Access Files on the CF/SD Card

Click the **My Device** icon on the Desktop then click the **System** icon.

A SD/CF card is used for permanent storage of the VX7 drivers, CAB files and utilities. It is also used for registry content back up.

CAB files, when executed, are not deleted.

Note: Always perform a warm reset (Start / Run / Warmboot) when exchanging one card for another.

VX7 Utilities

The following files are pre-loaded.

LAUNCH.EXE

Launch works in coordination with registry settings to allow drivers or applications to be loaded automatically into DRAM at system startup. Registry settings control what gets launched; see the App Note for information on these settings. For examples, you can look at the registry key

HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist

Launch will execute .CAB files, .BAT files, or .EXE files.

App Note

All applications to be installed into persistent memory must be in the form of Windows CE CAB files. These CAB files exist as separate files from the main installation image, and are copied to the CE device using ActiveSync, or using a CompactFlash ATA card. The CAB files are copied from ATA or using ActiveSync Explore into the folder System, which is the persistent storage virtual drive. Then, information is added to the registry, if desired, to make the CAB file auto-launch at startup.

The registry information needed is under the key HKEY_LOCAL_MACHINE \ Software \ LXE \ Persist, as follows. The main subkey is any text, and is a description of the file. Then three mandatory values are added:

FileName is the name of the CAB file, with the path (usually \System).

Installed is a DWORD value of 0, which changes to 1 once auto-launch installs the file.

FileCheck is the name of a file to look for to determine if the CAB file is installed. This will be the name of one of the files (with path) installed by the CAB file. Since the CAB file installs into DRAM, when memory is lost this file is lost, and the CAB file must be reinstalled.

There are three optional fields that may be added:

1. Order is used to force a sequence of events. Order=0 is first, and Order=99 is last. Two items which have the same order will be installed in the same pass, but not in a predictable sequence.
2. Delay is used to add a delay after the item is loaded, before the next is loaded. The delay is given in seconds, and defaults to 0 if not specified. If the install fails (or the file to be installed is not found), the delay does not occur.
3. PCMCIA is used to indicate that the file (usually a CAB file) being loaded is a radio driver, and the PCMCIA slots should be started after this file is loaded. By default, the PCMCIA slots are off on powerup, to prevent the “Unidentified PCMCIA Slot” dialog from appearing. Once the drivers are loaded, the slot can be turned on. The value in the PCMCIA field is a DWORD, representing the number of seconds to wait after installing the CAB file, but before activating the slot (a latency to allow the thread loading the driver to finish installation). The default value of 0 means the slot is not powered on. The default values for the default radio drivers (listed below) is 1, meaning one second elapses between the CAB file loading and the slot powering up.

The auto-launch process proceeds as follows:

- The launch utility opens the registry database and reads the list of CAB files to auto-launch.
- First it looks for FileName to see if the CAB file is present. If not, the registry entry is ignored. If it is present, and the Installed flag is not set, auto-launch makes a copy of the CAB file (since it gets deleted by installation), and runs the Microsoft utility WCELOAD to install it.

- If the Installed flag is set, auto-launch looks for the FileCheck file. If it is present, the CAB file is installed, and that registry entry is complete. If the FileCheck file is not present, memory has been lost, and the utility calls WCELOAD to reinstall the CAB file.
- Then, the whole process repeats for the next entry in the registry, until all registry entries are analyzed.
- To force execution every time (for example, for AUTOEXEC.BAT), use a FileCheck of “dummy”, which will never be found, forcing the item to execute.
- For persist keys specifying .EXE or .BAT files, the executing process is started, and then Launch will continue, leaving the loading process to run independently. For other persist keys (including .CAB files), Launch will wait for the loading process to complete before continuing. This is important, for example, to ensure that a .CAB file is installed before the .EXE files from the .CAB file are run.
- Note that the auto-launch process can also launch batch files (*.BAT), executable files (*.EXE), registry setting files (*.REG), or sound files (*.WAV). The mechanism is the same as listed above, but the appropriate CE application is called, depending on file type.

Note: Registry entries may vary depending on software revision level and options ordered with the VX7.

LAUNCH.EXE and Persistent Storage

If any of the following directories are created in the System folder, Launch automatically copies all of the files in these directories to the respective folder on the installed CF/SD drive:

- AppMgr
- Desktop
- Favorites
- Fonts
- Help
- Programs
- Recent

*Note: Files in the Startup folder are executed, but only from **System > Startup**. They are not copied to another folder.*

REGEDIT.EXE

Registry Editor – Use caution when editing the Registry and make a backup copy of the registry before changes are made.

REGLOAD.EXE

Double-tapping a registry settings file (e.g. REG) causes RegLoad to open the file and make the indicated settings in the registry. This is similar to how RegEdit works on a desktop PC. The .REG file format is the same as on the desktop PC.

REGDUMP.EXE

Registry dump – Saves a copy of the registry as a text file. The file, REG.TXT, is located in the root folder.

Note: The REG.TXT file is not saved in persistent storage. To use the REG.TXT file as a reference in the event of a coldboot, copy the file to the System folder on the VX7 or store a copy of the REG.TXT file on a PC.

WARMBOOT.EXE

Double click this file to warm boot the computer (i.e., all RAM is preserved). It automatically saves the registry before rebooting which means configuration changes are not lost.

WAVPLAY.EXE

Double tapping a sound file (e.g. WAV) causes WavPlay to open the file and run it in the background.

VX7 Command-line Utilities

Command line utilities can be executed by **Start > Run >** [program name].

COLDBOOT.EXE

Command line utility which performs a cold boot (all RAM is erased).

Passwords are lost upon cold boot. If a password is set, that password must be entered to begin the cold boot power cycle process.

PrtScrn.EXE

Command line utility which performs a screen print and saves the file in .BMP format in the \System folder. Tap **Start > Run** and type **prtscrn** and tap **OK**, or press Enter. There is a 10 second delay before the screen print is made. The device beeps and the screen captured file (*scrnnnn*.bmp) is placed in the \System folder. The numeric filename is incremented by 1 each time the PrtScrn function is activated. The command is not case-sensitive.

Desktop

Note: For general use instruction, please refer to commercially available Windows CE user's guides or the Windows on-line Help application installed in the mobile device.

The VX7 Desktop appearance is similar to that of a desktop PC running a Windows operating system.

At the bottom of the screen is the Start button. Tapping the Start Button causes the Start Menu to pop up. It contains the standard Windows menu options: Programs, Favorites, Documents, Settings, Help, and Run.

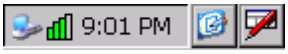
Desktop Icons

At a minimum, the desktop displays icons for My Device, Internet Explorer and the Recycle Bin. Following are a few of the other icons that may be on the VX7 Desktop. Please Contact Technical Assistance for the latest updates and upgrades for your operating system.

Icon	Function
My Device	Access files and programs.
Recycle Bin	Storage for files that are to be deleted.
Bluetooth	Discover and then pair with nearby discoverable Bluetooth devices.
My Documents	Storage for downloaded files / applications.
Internet Explorer	Connect to the Internet/intranet
Summit Client Utility	Used for accessing the appropriate wireless configuration, SCU (Summit Client Utility).
eXpress Scan	The eXpress Scan utility allows an administrator to scan barcodes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the VX7. eXpress Scan uses barcodes created with eXpress Config.

Icon	Function
LXE RFTerm	RFTerm is an optional terminal emulation program for the VX7. When RFTerm is installed, this icon is displayed on the desktop.
Remote Desktop Connection	A shortcut to the Remote Desktop Connection utility.
Avalanche	Wavelink® Avalanche Mobility Center™ (Avalanche MC) is a remote client management system that is designed to distribute software and configuration updates to monitored devices, including the VX7. The enabler for Wavelink Avalanche is loaded on the VX7 but not installed. When the enabler is installed this icon is displayed on the desktop.
TelnetCE	The demo version of Wavelink Telnet CE is installed on all devices. Please Contact Technical Assistance for licensing information. When installed, license details are maintained in the Wavelink tab in the License Viewer control panel.
Java	Tapping the desktop icon displays information on the Java version installed. Files can be accessed by tapping **Start > Programs > JEM-CE**. Doubletap the EVM icon to open the EVM Console. A folder of Java examples and Plug-ins is also installed with the Java option. Honeywell does not support Java applications running on the mobile device.
	Start button. Access programs, select from the Favorites listing, documents last worked on, change/view settings for the control panel or taskbar, on-line help or run programs.

Taskbar



The number and type of icons displayed are based on the device type, installed options and configuration of the VX7.

My Device Folders

Folder	Description	Preserved upon Reboot?
Application Data	Data saved by running applications	No
My Documents	Storage for downloaded files / applications	No
Network	Mounted network drive	No
Program Files	Applications	No
System	Internal CF/SD Card (CAB file storage)	Yes
Storage Card or SD Card	Additional optional storage space	Yes
Temp	Location for temporary files	No
Windows	Operating System in Secure Storage	No

Wavelink Avalanche Enabler (Optional)

Note: If the user is NOT using Wavelink Avalanche to manage their mobile device, the Enabler should not be installed on the mobile device(s).

The following features are supported by the Wavelink Avalanche Enabler when used in conjunction with the Avalanche Manager.

After configuration, Enabler files are installed upon initial bootup and after a hard reset. Network parameter configuration is supported for:

- IP address: DHCP or static IP
- RF network SSID
- DNS hosts (primary, secondary, tertiary)
- Subnet mask
- Enabler update

Related Manual: *Using Wavelink Avalanche*

The VX7 has the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the System folder on CE devices. The installation application must be run manually the first time Avalanche is used.

After the installation application is manually run, a reboot is necessary for the Enabler to begin normal performance. Following this reboot, the Enabler will by default be an auto-launch application. This behavior can be modified by accessing the *Avalanche Update Settings* panel through the *Enabler Interface*.

The designation of the mobile device to the Avalanche CE Manager is LXE_VXC, LXE_VX7 or LXE_VX7SD.

Devices manufactured before October 2006 must have their drivers and system files upgraded before they can use the Avalanche Enabler functions. Please Contact Technical Assistance for details on upgrading the mobile device baseline.

Internet Explorer

Start > Programs > Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the “?” button to access Internet Explorer Help.

Start Menu Program Options

The following list represents the factory default program installation. Your system may contain different items from those shown below, based on the software and hardware options purchased.

Communication	Stores Network communication options
ActiveSync	Transfer files between a VX7 and a desktop computer
Connect	Run this command after setting up a connection
Start (or Stop) FTP Server	Begin / end connection to FTP server
Command Prompt	The command line interface in a separate window
eXpress Scan	Option. Requires Wavelink Avalanche option eXpress Config.
Internet Explorer	Access web pages on the Internet/Intranet
Java	Optional
Media Player	Digital media player for movie and audio files.
Microsoft File Viewers[1]	View downloaded files
Excel Viewer	View Excel 97 and newer documents
Image Viewer	View BMP, JPEG and PNG images
PDF Viewer	View Adobe Acrobat documents
Word Viewer	View Word 97 and newer documents and RTF files
Microsoft WordPad	Opens an ASCII notepad
Remote Desktop Connection	Log on to a Windows Terminal Server
RFTerm	Option. Terminal emulation application.
Settings	Access to all Control Panels, a shortcut to the Network and Dialup Control Panel and access to Taskbar options.
Summit	Set Summit radio / network parameters
Transcriber	Enter data using the stylus on the touch screen
Wavelink Avalanche	Option. Remote management for networked devices
Windows Explorer	File management program

- If installed, RFTerm runs automatically at the conclusion of each reboot.
- If installed and enabled, AppLock runs automatically at the conclusion of each reboot.
- The wireless client connects automatically during each reboot.
- Bluetooth re-connects to nearby paired devices automatically at the conclusion of each reboot.
- If installed and pre-configured, Wavelink Avalanche connects remotely and downloads updates automatically during each reboot.

[1] The Microsoft File Viewers cannot display files that have been password protected.

Communication

Start > Programs > Communication

ActiveSync

Start FTP Server / Stop FTP Server

Start > Programs > Communication > Start (or Stop) FTP Server

These shortcuts call the Services Manager to start and stop the FTP server. The server defaults to Off (for security) unless it is explicitly turned on from the menu.

Summit

Start > Programs > Summit > SCU

Use this option to set up radio client profiles.

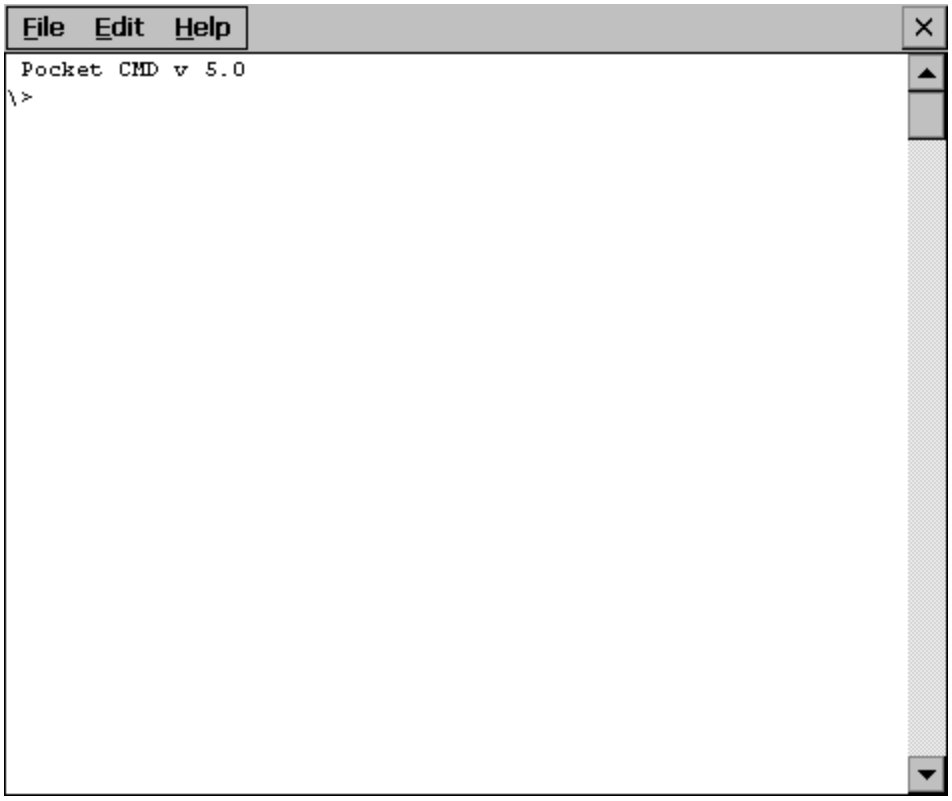
The Summit Control Panel can also be accessed by doubletapping the Summit icon in the taskbar or on the desktop.

Certs

The Certs option displays a readme file containing details on how the Summit Configuration Utility (SCU) handles certificates for WPA authentication.

Command Prompt

Start > Programs > Command Prompt



Type **help cmd** at the command prompt to view valid Pocket PC (Console) commands.

Exit the command prompt by typing **exit** at the command prompt or tap **File > Close.**

eXpress Scan

The eXpress Scan utility allows an administrator to scan barcodes to provide the initial network and Avalanche Mobile Device Server address configuration. This eliminates the need to edit radio parameters manually on the VX7.

eXpress Scan uses barcodes created with eXpress Config.

Internet Explorer

Start > Programs > Internet Explorer

This option requires a radio card and an Internet Service Provider. There are a few changes in the Windows CE version of Internet Explorer as it relates to the general desktop Windows PC Internet Explorer options. Tap the ? button to access Internet Explorer Help.

Media Player

Start > Programs > Media Player

There are few changes in the Windows CE version of Media Player as it relates to the general desktop Windows PC Microsoft Media Player options.

After the Media Player application is running, click the ? button to access Media Player Help.

Microsoft File Viewers

The following applications are included:

- Word Viewer
- Excel Viewer
- PDF Viewer
- Image Viewer

Note: The viewer applications allow viewing documents, but not editing them.

Microsoft WordPad

Start > Programs > Microsoft WordPad

Create and edit documents and templates in WordPad, using buttons and menu commands that are similar to those used in the desktop PC version of Microsoft WordPad.

By default WordPad files are saved as .PWD files. Documents can be saved in other formats e.g. .RTF or .DOC.

Tap the ? button to access WordPad Help.

Remote Desktop Connection

Start > Programs > Remote Desktop

There are few changes in the Windows CE version of Remote Desktop as it relates to the general desktop Windows PC Microsoft Remote Desktop options.

If installed, Remote Desktop on the VX7 can be accessed by **Start > Programs > Remote Desktop**.

Select a computer from the drop down list or enter a host name and tap the Connect button.

Tap the Options >> button to access the General, Display, Local Resources, Programs and Experience tabs. Tap the ? button to access Remote Desktop Connection Help.

Settings

Start > Settings

The Settings menu option may include the following:

Control Panel	All control panels
Network and Dialup Connections	Shortcut to control panel. Connect to a network, create a new connection, and adjust parameters for client connections.
Taskbar	Set Taskbar parameters

Transcriber

To make changes to the Transcriber application, tap the keyboard icon in the status bar. Select Transcriber from the pop-up menu. Then open the Input control panel and tap the Options button. Transcriber Options (**Start > Settings > Control Panel > Input Panel**) are available only when Transcriber is selected as the active input method. Tap the "?" button or the Help button to access Transcriber Help.

Windows Explorer

Start > Programs > Windows Explorer

There are a few changes in the Windows CE version of Windows Explorer as it relates to the general desktop PC Windows Explorer options. Tap the "?" button to access Windows Explorer Help.

Taskbar

Start > Settings > Taskbar

There are a few changes in the Windows CE version of Taskbar as it relates to the general desktop PC Windows Taskbar options.

When the taskbar is auto hidden, press the Ctrl key then the Esc key to make the Start button appear.

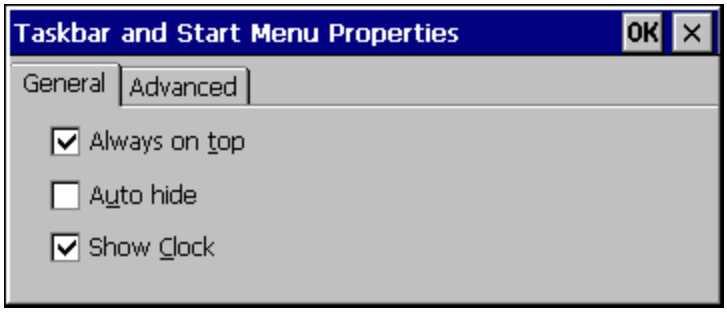
Clicking the Taskbar option on the Settings menu displays the Taskbar General tab and the Taskbar Advanced tab.

See Also: "Taskbar Icons"

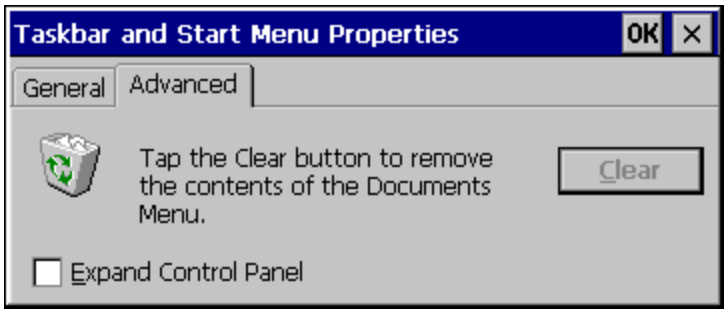
General Tab

Factory Default Settings

Always on Top	Enabled
Auto hide	Disabled
Show Clock	Enabled



Advanced Tab



Expand Control Panel

Tap the checkbox to have the Control Panel folders appear in drop down menu format from the **Settings > Control Panel** menu option.

Clear Contents of Document Folder

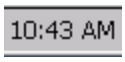
Tap the Clear button to remove the contents of the Document folder.

Taskbar Icons

As VX7 devices and applications open and change state, icons are placed in the Taskbar. In most cases, tapping the icon in the Taskbar opens the related application.

Refer to **Start > Help** for an explanation of standard Windows CE taskbar icons.

Following are a few of the VX7 unique taskbar icons that may appear in the Taskbar. These icons are in addition to the Windows CE taskbar icons.

	Wireless Zero Config Inactive / Connected / Not Connected. Clicking on the icon opens the Wireless Zero Config utility.
	Bluetooth connected / disconnected. Clicking the icon opens the Bluetooth control panel.
	ActiveSync Connection
	Cerdisp connected (displayed when LXEConnect is connected)
	Summit Client signal indicator no signal / excellent signal. Clicking on the icon opens the Summit Client Utility.
	Current time. Clicking the time display opens the Date/Time control panel.
	AppLock switchpad.
	Input method, keyboard / input panel / transcriber
	CapsLock active

VX7 OS Upgrade

Introduction

Depending on the size of the operating system, the total time required for a successful upgrade may require several minutes.

The OS upgrade files are unique to your VX7 physical configuration and date of manufacture. OS upgrade files designed for one device configuration should not be used on a different device configuration.

Preparation

- Please Contact Technical Assistance to get the **OS upgrade files**.
- Use ActiveSync to back up VX7 user files and store them elsewhere before beginning an upgrade on the VX7.
- Maintain an uninterrupted AC/DC power source to the VX7 throughout this process.
- The SD / CF card with the OS and systems files must be present for the VX7 to boot. Removal or installation of SD or CF cards should be performed on a clean, well-lit surface.
- Always perform OS updates when the VX7 has a dependable external power source connected to the VX7.

Procedure

1. Verify a dependable power source is applied to the VX7 and will stay connected during the upgrade procedure.
2. Establish an ActiveSync connection between the VX7 and a desktop/laptop computer.
3. Download the OS files from the desktop/laptop to the VX7's System folder.
4. During the file copy process to the VX7 System folder, when asked “Overwrite ?”, select Yes to All.
5. Review the files that were downloaded to the System folder.
6. Restart the VX7.
7. Disconnect from ActiveSync.
8. When the OS finishes loading, check the OS update version by selecting **Start > Settings > Control Panel > About > Software** tab.

The touch screen may require calibration, however most Windows OS versions save the calibration data, eliminating the need to calibrate.

Contact Technical Assistance for re-imaging options if the VX7 won't boot up after the upgrade is finished.

ActiveSync

Introduction

Once a relationship (partnership) has been established with Connect (on a desktop computer), ActiveSync will synchronize using the wireless link, serial port, or USB on the VX7.

Requirement : ActiveSync (version 4.5 or higher for **Windows XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC is available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

Using Microsoft ActiveSync, you can synchronize information on your desktop computer with the VX7 and vice versa. Synchronization compares the data on your mobile device with your desktop computer and updates both with the most recent data.

For example, you can:

- Back up and restore your device data.
- Copy (rather than synchronize) files between your device and desktop computer.
- Control when synchronization occurs by selecting a synchronization mode. For example, you can synchronize continually while connected to your desktop computer or only when you choose the synchronize command.

By default, ActiveSync does not automatically synchronize all types of information. Use ActiveSync Options to specify the types of information you want to synchronize. The synchronization process makes the data (in the information types you select) identical on both your desktop computer and your device.

When installation of ActiveSync is complete on your desktop computer, the ActiveSync Setup Wizard begins and starts the following processes:

- connect your device to your desktop computer,
- set up a partnership so you can synchronize information between your device and your desktop computer, and
- customize your synchronization settings.

Because ActiveSync is already installed on your device, your first synchronization process begins automatically when you finish setting up your desktop computer in the ActiveSync wizard. For more information about using ActiveSync on your desktop computer, open ActiveSync, then open ActiveSync Help.

Initial Setup

The initial setup of ActiveSync must be made via a USB or serial connection. When there is a Connect icon on the desktop, this section can be bypassed.

Partnerships can only be created using direct serial or a USB cable connection.

After the partnerships are established, ActiveSync communication can be initiated using:

- USB
- Serial
- Wireless

Connect via USB

The default connection type is **USB Client**

To change the connection type or to verify it is set to USB, select

Start > Settings > Control Panel > PC Connection

Tap the Change button. From the popup list, choose

USB Client

This will set up the mobile device to use the USB port. Tap OK and ensure the check box for “Allow connection with desktop computer when device is attached” is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

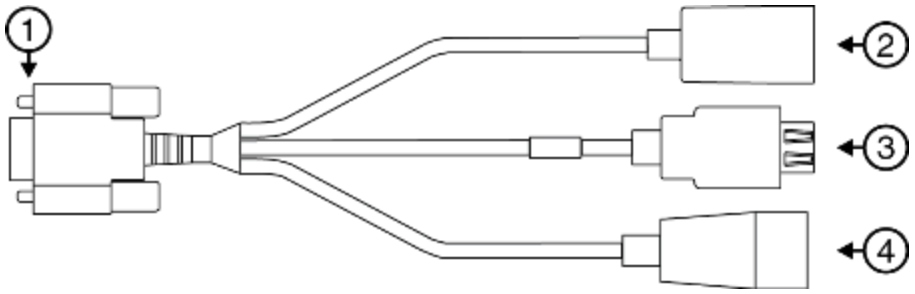
DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Connect the correct cable to the PC (the host) and the mobile device (the client) as detailed below. USB will start automatically when the USB cable is connected, not requiring you to select “Connect” from the start menu.

Cables for USB ActiveSync Connection:

9000075CABLE - VX7 Dongle cable provides USB type B connector. Also requires a user provided **standard USB cable** with type A plug for PC/Laptop USB port and type B plug for VX7dongle cable USB type B client port

- D15 connector (labeled as 1 below) connects to the ETHERNET/USB port on the VX7
- Plug the type B end of the standard USB cable plug into the USB host dongle cable (labeled as 4 below).
- The USB type A connector on the standard cable connects to a USB port on a PC or laptop.
- The Ethernet (port #2) and USB client (port #3) connectors on the dongle cable do not need to be connected.



Serial Connection

The connection type must be changed to **Serial 1 @ 57600** or **Serial 3 @ 57600** depending on which serial port on the VX7 is used.

To change the connection type select

Start > Settings > Control Panel > PC Connection

Tap the Change button. From the popup list, choose

Serial 1 @ 57600 or **Serial 3 @ 57600**

This will set up the mobile device to use the serial port. Tap OK and ensure the check box for "Allow connection with desktop computer when device is attached" is checked.

Tap OK to return to the Control Panel. If desired, any control panel windows may be closed.

Select **Start > Settings > Scanner** and ensure the integrated scanner is set to a port that is NOT the same as the ActiveSync port.

Connect the correct cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the client (**Start > Programs > Communications > Connect**).

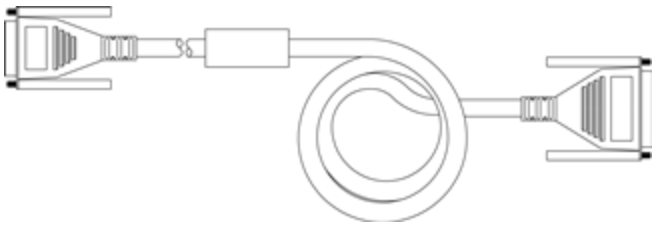
Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Cable for Serial ActiveSync Connection

Serial ActiveSync

9000054CABLE, RS-232 9 Pin to 9 Pin, VX7 Serial port to PC/Laptop serial port

- Connect one end of the cable to the COM port (labeled COM1 or COM2/3) on the VX7
- Connect the other end to a COM port on a PC or laptop.



Wireless Connection

Note: You must establish a partnership with a desktop computer prior to running ActiveSync on the mobile device. The initial partnership must be done using direct serial or USB cable connection.

Once the relationship is established using the serial port, the ActiveSync link in the Start Menu gives a choice of connections, one of which is Network.

Select **Start > Settings > Programs > Communication > ActiveSync**. From the popup list, choose Network and then tap the Connect button.

VX7 with Disabled Touch Screen

For a VX7, the touch screen can be disabled. It may be easier to configure the VX7 using ActiveSync and LXEConnect rather than using the VX7 keyboard only.

Synchronizing from the Mobile Device

To synchronize using a wireless LAN card, you must have set up ActiveSync on your desktop computer and completed the first synchronization process before you initiate synchronization from your device.

To initiate synchronization from your VX7, tap **Start > Programs > Communication > ActiveSync** to begin the process.

Tap **Sync** to connect and synchronize. View synchronization status.

Tap **Tools** to synchronize or change synchronization settings. View connection status.

Tap **Stop** to stop synchronization.

Tap **Start > Help** for context-sensitive help.

Explore

From the ActiveSync Dialog on the Desktop PC, tap the Explore button, which allows you to explore the mobile device from the PC side, with some limitations. You can copy files to or from the mobile device by drag-and-drop. You will not be allowed to delete files or copy files out of the \Windows folder on the mobile device. (Technically, the only files you cannot delete or copy are ones marked as system files in the original build of the Windows image. This, however, includes most of the files in the \Windows folder).

Backup Data Files using ActiveSync

Use the following information to backup data files from the mobile device to a desktop or laptop PC using the appropriate cables and Microsoft's ActiveSync.

Prerequisites

A partnership between the mobile device and ActiveSync has been established.

Serial Port Transfer

- A desktop or laptop PC with an available serial port and a mobile device with a serial port. The desktop or laptop PC must be running Windows XP or greater.
- Null modem cable with all control lines connected. Use the null modem cable part number listed in Connect via Serial.

USB Transfer

- A desktop or laptop PC with an available USB port and a mobile device with a USB port. The desktop or laptop PC must be running Windows XP or greater.
- Use the specific USB cable as listed in Connect Via USB.

Connect

Connect the modem cable to the PC (the host) and the mobile device (the client). Select "Connect" from the Start Menu on the mobile device (**Start > Programs > Communications > Connect**).

Note: Run "Connect" when the "Get Connected" wizard on the host PC is checking COM ports to establish a connection for the first time.

Note: USB synchronization will start automatically when the cable is connected, not requiring you to select "Connect" from the Start menu.

Disconnect

USB Connection

- Disconnect the cable from the mobile device.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

DO NOT PUT THE MOBILE DEVICE INTO SUSPEND WHILE CONNECTED VIA USB. The device will be unable to connect to the host PC when it resumes operation.

Serial Connection

- Disconnect the cable from the mobile device.
- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Network Connection

- Put the mobile device into Suspend.
- Tap the status bar icon in the lower right hand corner of the status bar. Then tap the Disconnect button.

Cold Boot and Loss of Host Re-connection

ActiveSync assigns a partnership between a client and a host computer. A partnership is defined by two objects – a unique computer name and a random number generated when the partnership is first created. An ActiveSync partnership between a unique client can be established to two hosts.

When the mobile device is cold booted, the random number is deleted – and the partnership with the last one of the two hosts is also deleted. The host retains the random numbers and unique names of all devices having a partnership with it. Two clients cannot have a partnership with the same host if they have the same name. (**Control Panel > System > Device Name**)

If the cold booted mobile device tries to reestablish the partnership with the same host PC, a new random number is generated for the mobile device and ActiveSync will insist the unique name of the mobile device be changed. If the mobile device is associated with a second host, changing the name will destroy that partnership as well. This can cause some confusion when re-establishing partnerships with hosts.

ActiveSync Help

ActiveSync on the host says that a device is trying to connect, but it cannot identify it

One or more control lines are not connected. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

If the VX7 is connected to a PC by a cable, disconnect the cable from the VX7 and reconnect it again.

Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

See Also: "Cold Boot and Loss of Host Reconnection".

ActiveSync indicator on the host (disc in the toolbar tray) turns green and spins as soon as you connect the cable, before tapping the Connect icon (or REPLLOG.EXE in the Windows directory).

One or more control lines are tied together incorrectly. This is usually a cable problem, but on a laptop or other device, it may indicate a bad serial port.

ActiveSync indicator on the host turns green and spins, but connection never occurs

Baud rate of connection is not supported or detected by host. Check that the correct connection is selected (Serial or USB "Client" if this is the initial ActiveSync installation).

-or-

Incorrect or broken data lines in cable.

ActiveSync indicator on the host remains gray

Solution 1: ActiveSync icon on the PC does not turn green after connecting USB cable from VX7.

1. Disconnect VX7 USB cable from PC.
2. Suspend/Resume or Restart the VX7.
3. In **ActiveSync > File > Connection Settings** on PC disable Allow USB Connections and click OK.
4. Re-enable Allow USB Connections on the PC and click OK.
5. Reconnect USB cable from VX7 to PC.

Solution 2: The host doesn't know you are trying to connect. May mean a bad cable, with no control lines connected, or an incompatible baud rate. Try the connection again, with a known good cable.

Testing connection with a terminal emulator program, or a serial port monitor

You can use HyperTerminal or some other terminal emulator program to do a rough test of ActiveSync. Set the terminal emulator to 8 bits, no parity, 1 stop bits, and the same baud rate as the connection on the CE device. After double-tapping REPLLOG.EXE on the CE device, the word "CLIENT" appears on the display in ASCII format. When using a serial port monitor, you see the host echo "CLIENT", followed by "SERVER". After this point, the data stream becomes straight (binary) PPP.

Configuring the VX7 with LXEConnect

LXEConnect allows a user to view the VX7 screen remotely from a PC using an ActiveSync connection:

Requirement : ActiveSync (version 4.5 or higher for **Windows XP** desktop/laptop computers) must be resident on the host (desktop/laptop) computer. **Windows Mobile Device Center** is required for a **Windows Vista/Windows 7** desktop/laptop computer. ActiveSync and Windows Mobile Device Center for the PC are available from the Microsoft website. Follow their instructions to locate, download and install ActiveSync or Windows Mobile Device Center on your desktop computer.

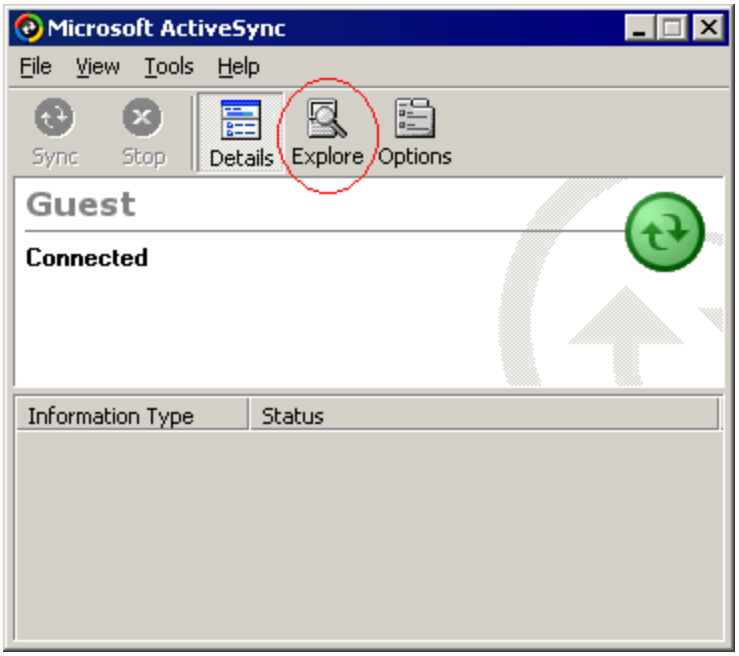
Note: For readability in this section, ActiveSync will be used in instructions and explanations. If you have a Windows Vista or Windows 7 operating system on your desktop/laptop, replace ActiveSync with Windows Mobile Device Center.

ActiveSync is already installed on the VX7. The VX7 is preconfigured to establish a USB ActiveSync connection to a PC when the proper cable is attached to the VX7 and the PC.

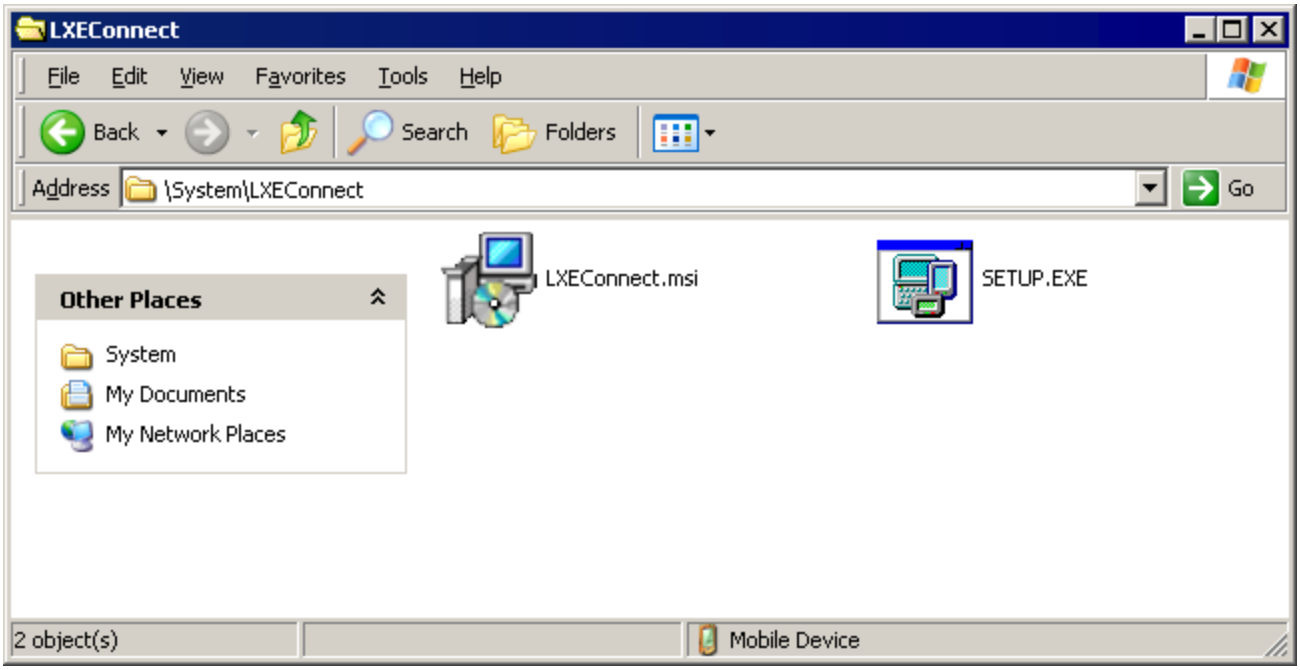
If the VX7 uses a serial port for ActiveSync, it will be necessary to configure the VX7 to use the serial port. Complete details on the proper cables and port configuration are included in Initial Setup.

Install LXEConnect

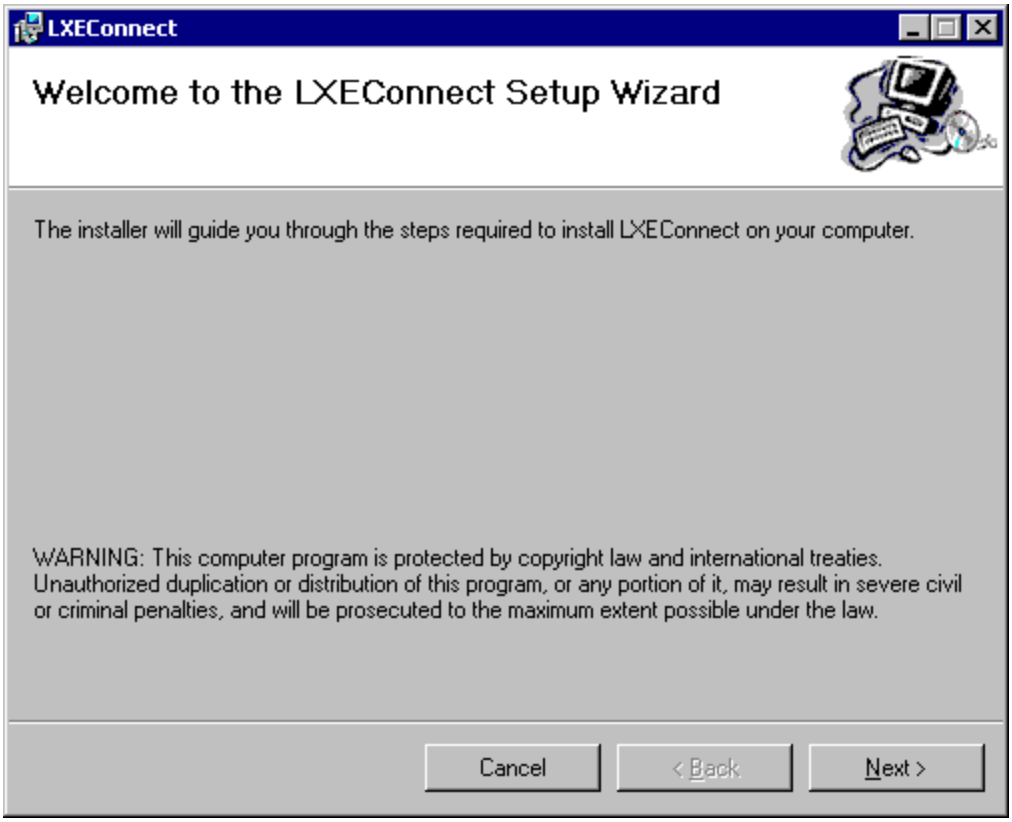
1. Install Microsoft ActiveSync on a PC with a USB port. For details, please see Initial Setup.
2. Power up the VX7.
3. Connect the VX7 to the PC using the proper connection cable. Once connected, the ActiveSync dialog box appears. If using the USB connection, the ActiveSync connection is automatically established. If using a serial connection, it is necessary to initiate the connection from the VX7.
4. Select “No” for partnership when prompted. Dismiss any ActiveSync dialog boxes warning a partnership is not set up. It is not necessary to establish a partnership to use LXEConnect. However, if a partnership is desired for other reasons, one may be established now. More details on partnerships are included in ActiveSync Help.
5. When the ActiveSync screen appears, select Explore.



6. An explorer window is displayed for the VX7. Browse to the \System\LXEConnect folder. Contact Technical Assistance for the necessary files if this folder is not present.



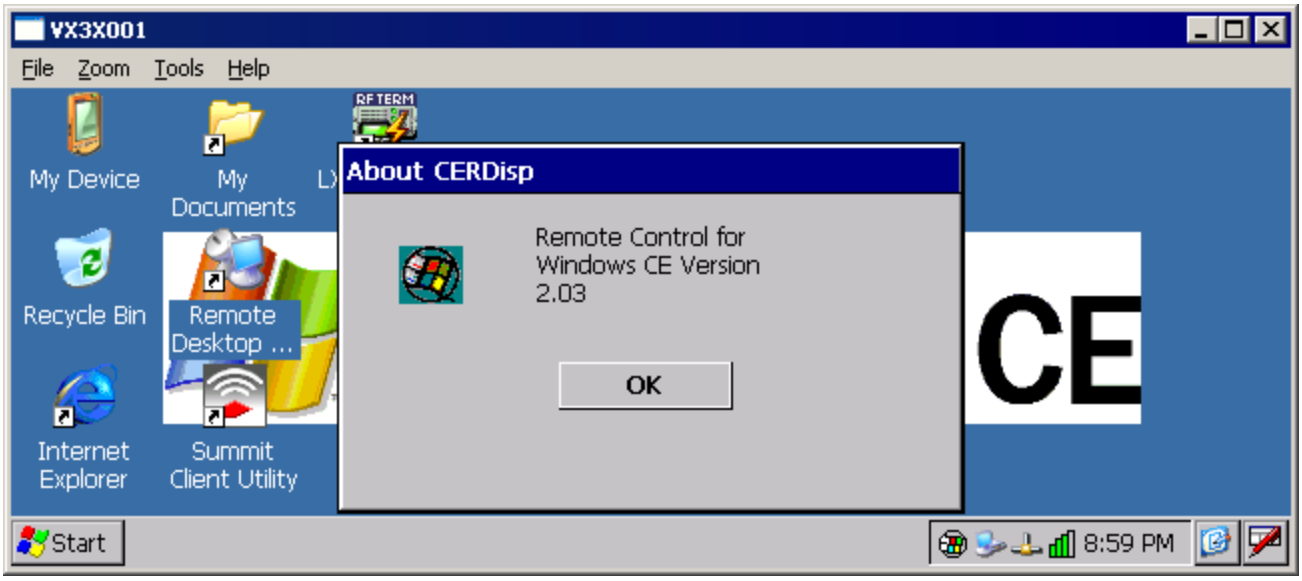
7. Select and copy the LXEConnect.msi and Setup.exe files from the VX7 to the user PC. Note the location chosen for the files.
8. Close the ActiveSync explorer dialog box. Do not disconnect the VX7 ActiveSync connection.
9. Execute the setup.exe file that was copied to the user PC. This setup program installs the LXEConnect utility.


LXEConnect
Welcome to the LXEConnect Setup Wizard
The installer will guide you through the steps required to install LXEConnect on your computer.
WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.
Cancel
< Back
Next >

10. Follow the on screen installation prompts. The default installation directory is C:\Program Files\LXE\LXEConnect.
11. When the installation is complete, create a desktop shortcut to the following file: C:\Program Files\LXE\LXEConnect\LXEConnect.exe. If a different directory was selected during installation, please substitute the appropriate directory.
12. LXEConnect is now installed and ready to use.

Using LXEConnect

1. If an ActiveSync connection has not been established, connect the VX7 to the PC.
2. Double-click the LXEConnect icon that was created on the desktop.
3. LXEConnect launches.



4. Click the OK button to dismiss the About CERDisp dialog box. on the VX7 desktop by clicking the OK button in the LXEConnect window on the PC desktop. The dialog box automatically times out and disappears after approximately 30 seconds.

5. The VX7 can now be configured from the LXEConnect window. Input from the PC's mouse and keyboard are recognized as if they were attached to the VX7.
6. When the remote session is completed, terminate the LXEConnect program by selecting **File > Exit** or clicking on the X in the upper right hand corner to close the application, then disconnect the ActiveSync cable.

Note: After using LXEConnect, the VX7 cannot go into Suspend mode until after a warmboot. If using Power Management on a VX7, always warmboot the VX7 when finished using LXEConnect.

Control Panel

Start > Settings > Control Panel or My Device > Control Panel link

Note: Change the font displayed on the touch screen by choosing Start > Settings > Control Panel > Keyboard and then the Key map dropdown list.

Tap the ? button for Help when changing VX7 Control Panel options.

Option	Function
About	Software, hardware, versions and network IP. No user intervention allowed.
Accessibility	Customize the way the keyboard, audio, display or mouse function for users with hearing or viewing difficulties.
Administration	AppLock Administration utility.
Bluetooth	Set the parameters for Bluetooth device connections.
Certificates	Manage digital certificates used for secure communication.
Date/Time	Set Date, Time, Time Zone, and Daylight Savings.
Device Management	Connection setup for Microsoft Systems Management Server.
Dialing	Connection setup for modem attached to COM port or CompactFlash slot.
Display	Set background graphic and scheme. Set touch screen and keypad backlight properties and timers.
Input Panel	Select the current key / data input method. Select custom key maps.
Installed Programs	View the list of installed programs.
Internet Options	Set General, Connection, Security, Privacy, Advanced and Popups options for Internet connectivity.
Keyboard	Select a Key Map (or font). Set key repeat delay and key repeat rate.
KeyPad	Configure KeyMap keys, RunCmd and LaunchApp.
License Viewer	Displays license information for installed licensed applications.
Mixer	Adjust the input and output parameters – volume, sidetone, and record gain, for headphone, software and microphone.
Mouse	Set the double-tap sensitivity for stylus taps on the touch screen.
MX3X-VXC Options	Set various device specific configuration options.
Network and Dial Up Options	Set network driver properties and network access properties.
Network Capture	Set network logging options.
Owner	Set the mobile device owner details (name, phone, etc.). Enter notes. Enable / disable Owner display parameters. Enter Network ID for the device – user name, password, domain.
Password	Set OS access password properties for signon and/or screen saver.
PC Connection	Control the connection between the mobile device and a local desktop or laptop computer.

Option	Function
PCMCIA	Manage cards in card slots and IntATA card slot.
Power	Set Power scheme properties. Review device status and properties.
Regional Settings	Set appearance of numbers, currency, time and date based on country region and language settings.
Remove Programs	This panel has been replaced by Installed Programs
Scanner	Scan Wedge utility. Set scanner key wedge, scanner port, and imager LED illumination options. Assign baud rate, parity, stop bits and data bits for COM1 port. Assign scanned barcode data manipulation parameters.
Stylus	Set double-tap sensitivity properties and/or calibrate the touch panel.
System	Review System and Computer data and revision levels. Adjust Storage and Program memory settings. Enter device name and description. Review copyright notices.
Terminal Server Client Licenses	Select a server client license from a drop down list.
Volume and Sounds	Enable / disable volume and sounds. Set volume parameters and assign sound WAV files to events.
WiFi	Set the parameters for a Summit client.

About

Start > Settings > Control Panel > About

The data cannot be edited by the VX7 user on these panels.

Tab	Contents
Software	GUID, Windows CE Version, OAL Version, Bootloader Version, Compile Version, FPGA Version and Language. Language indicates any pre-installed Asian fonts.
Hardware	CPU Type, Codec Type, FPGA Version, Scanner type, Display, Flash memory, and DRAM memory
Versions	Revision level of software modules and .NET Compact Framework Version.
Network IP	Current network connection IP and MAC address. Only the first 2 network ports are shown (usually radio and ActiveSync).

Version window information is retrieved from the registry.

Version Tab and the Registry

Modify the Registry using the Registry Editor. Use caution when editing the Registry and make a backup copy of the registry before changes are made.

The registry settings for the Version tab are under HKEY_LOCAL_MACHINE \ Software \ LXE \ Version in the registry.

To add a user application to the Version panel, create a new string value under the HKLM\Software\LXE\Version key. The string name should be the Application name to appear in the Version window. The data for the value should be the version number to appear in the Version window .

Version strings can be equal to or less than 254 characters. Because the strings are displayed in a text box, any number can be accommodated, up to the 64K byte text box limitation.

Language and Fonts

The Software tab displays any fonts built into the OS image. The fonts built into the OS image are noted in the Language section of this tab:

- English only – No additional fonts are built into the OS
- Japanese
- Simplified Chinese
- Traditional Chinese
- Korean

The above listed Asian fonts are ordered separately and built-in to the OS image. Built-in fonts are added to registry entries and are available immediately upon startup. Thai, Hebrew, Arabic and Cyrillic Russian fonts are available in the (English only) default (extended) fonts.

When an Asian font is copied into the fonts folder on the /System folder; the font works for Asian web pages, the font works with RFTerm, the font does not work for Asian options in Regional Settings control panel, the font does not work for naming desktop icons with Asian names, the font does not work for third-party CE applications, the font does not work for some third-party MFC applications.

Identifying Software Versions

The Versions tab displays the versions of many of the software programs installed. Not all installed software installed on the mobile device is included in this list and the list varies depending on the applications loaded on the VX7. The Image line displays the revision of the system software installed. Refer to the last three digits to determine the revision level.

MAC Address

The Network IP tab displays the MAC address of the network card.

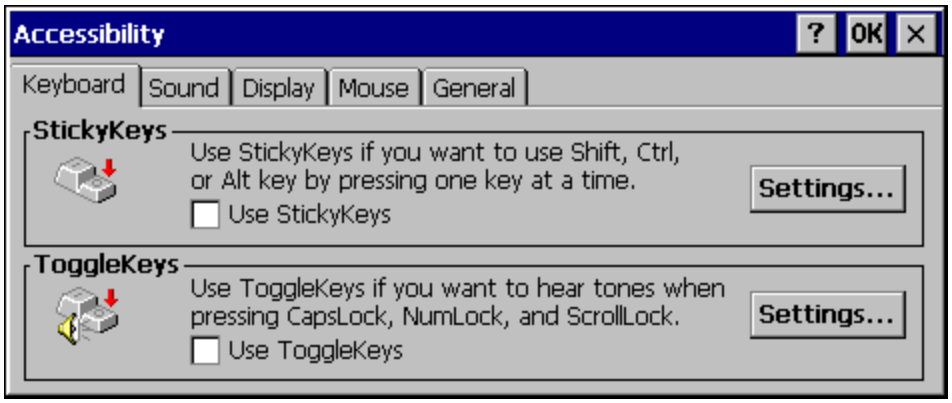
Accessibility

Start > Settings > Control Panel > Accessibility

Customize the way the VX7 keyboard, sound, display, mouse, automatic reset and notification sounds function. There are a few changes from general Windows desktop Accessibility options.

Note: StickyKeys and StickyKeys Settings on the Keyboard panel are disabled as this setting, when enabled, interferes with the VX7's assigned sticky key implementation.

Tab	Contents
Keyboard	Sticky Keys - Disabled. ToggleKeys - Disabled by default. Tap the *Use ToggleKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
Sound	SoundSentry is disabled by default. Tap the *Use SoundSentry* checkbox to enable this option. Tap the Settings button to view or change parameters.
Display	High Contrast is disabled by default. Tap the *Use High Contrast* checkbox to enable this option. Tap the Settings button to view or change parameters.
Mouse	MouseKeys is disabled by default. Tap the *Use MouseKeys* checkbox to enable this option. Tap the Settings button to view or change parameters.
General	Automatic reset is disabled by default. Tap the *Turn off accessibility features* checkbox to enable this option and use the dropdown option to assign a timer. Notification is enabled by default. Sounds are emitted when turning a feature on or off.



The following exceptions are due to a limitation in the Microsoft Windows CE operating system:

- If the ToggleKeys option is selected, please note that the ScrollLock key does not produce a sound as the CapsLock and NumLock keys do.
- If the SoundSentry option is selected, please note that ScrollLock does not produce a visual warning as the CapsLock and NumLock keys do.

Administration - AppLock

Start > Settings > Control Panel > Administration

Use this option to set parameters for computers intended to be used as dedicated, single or multiple application devices. In other words, only the application or feature specified in the AppLock configuration by the Administrator are available to the VX7 user.

VX7 devices with the AppLock feature are shipped to start up in Administration mode with no default password, and when the VX7 is started for the first time, the user has full access to the VX7 and no password prompt is displayed. After the Administrator specifies an application or applications to lock, assigns a password and the VX7 is rebooted (or the hotkey is pressed), the VX7 is then in end-user mode.

AppLock also contains a component which sets configuration parameters and application launch settings as specified by the Administrator.

AppLock is designed to be run on certified Windows CE based devices only. The AppLock program is part of the factory software load.

VX7 AppLock is setup by the Administrator by tapping **Start > Settings > Control Panel > Administration**.

Configuration parameters are specified by the AppLock Administrator for the mobile device end-user. AppLock is password protected by the Administrator.

End-user mode locks the end-user into the configured application or applications. The end user can still reboot the mobile device and respond to dialog boxes. The administrator-specified applications are automatically launched in the specified order and run in full screen mode when the device boots up.

When the mobile device is reset to factory default values, for example after a cold reset, the Administrator may need to reconfigure the AppLock parameters.

The assumption, in this chapter, is that the first user to power up a new mobile device is the system administrator.

Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other VX7 Control Panels.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application (see Auto Re-Launch) which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end-user mode to minimize the screen flicker.

AppLock is updated periodically as new options become available. Contact Technical Assistance for downloads and update availability.

Setup a New Device

VX7 devices with the AppLock feature are shipped to boot in Administration mode with no default password, thus when the VX7 is first booted, the user has full access to the device and no password prompt is displayed. After the administrator specifies the applications to lock, a password is assigned and the device is rebooted or the hotkey is pressed, the device switches to end-user mode.

Briefly, the process to configure a new device is as follows:

1. Connect an external power source to the device and press the Power button.
2. Adjust screen display, audio volume and other parameters if desired. Install accessories.
3. Tap **Start > Settings > Control Panel > Administration** icon.
4. Assign applications on the Control (single application) or Application (dual application) tab screen.
5. Assign a password on the Security tab screen.
6. Select a view level on the Status tab screen, if desired.
7. Tap OK
8. Press the hotkey sequence to launch AppLock and lock the configured application(s)
9. The device is now in end-user mode.

Administration Mode

Administration mode gives full access to the mobile device, hardware and software configuration options.

The administrator must enter a valid password (when a password has already been assigned) before access to Administration mode and configuration options are allowed. The administrator can configure the following options:

- Create/change the keystroke sequence to activate administrator access.
- Create/change the password for administrator access.
- Assign the name of the application, or applications, to lock.
- Select the command line of the application to lock.

In addition to these configuration options, the administrator can view and manage the status logs of AppLock sessions.

Administrator default values for this device:

Administrator Hotkey

Shift+Ctrl+A

Password

none

Application path and name

none

Application command line

none

End User Mode

End-user mode locks the end-user into the configured application or applications. The end user can still reboot and respond to dialog boxes. Each application is automatically launched and runs in full screen mode when the device boots up.

The user cannot unintentionally or intentionally exit the application nor can the end user execute any other applications. Normal application exit or switching methods and all Microsoft defined Windows CE key combinations, such as close (X) icon, File Exit, File Close, Alt-F4, Alt-Tab, etc. are disabled. The Windows CE desktop icons, menu bars, task bar and system trays are not visible or accessible. Task Manager is not available.

If the end-user selects File/Exit or Close from the applications menu bar, the menu is cleared and nothing else happens; the application remains active. Nothing happens when the end-user clicks on the Close icon on the application's title bar and the application remains active.

Note: A few applications do not follow normal procedures when closing. AppLock cannot prevent this type of application from closing, but is notified that the application has closed. For these applications, AppLock immediately restarts the application which causes the screen to flicker. If this type of application is being locked, the administrator should close all other applications before switching to end user mode to minimize the screen flicker.

Windows accelerator keys such as Alt-F4 are disabled.

Passwords

A password must be configured. If the password is not configured, a new device switches into Administration mode without prompting for a password. In addition to the hotkey press, a mode switch occurs if inaccurate information has been configured or if mandatory information is missing in the configuration.

There are several situations that display a password prompt after a password has been configured.

If the configured hotkey is pressed, the password prompt is displayed. In this case the user has 30 seconds to enter a password. If a valid password is not entered within 30 seconds, the password prompt is dismissed and the device returns to end-user mode.

All other situations that present the password prompt do not dismiss the prompt -- this is because the other situations result in invalid end-user operation.

These conditions include:

- If inaccurate configuration information is entered by the administrator, i.e. an application is specified that does not exist.
- If the application name, which is mandatory for end-user mode, is missing in the configuration.
- Invalid installation of AppLock (e.g. missing DLLs).
- Corrupted registry settings.

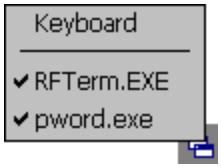
To summarize, if an error occurs that prevents AppLock from switching to user mode, the password will not timeout and AppLock will wait until the correct password is entered.

Forgotten password?

See: AppLock Help

End-User Switching Technique

Note: The touch screen must be enabled.



A checkmark indicates applications currently active or available for Launching by the user. When Keyboard is selected, the VX7 default input method (Input Panel, Transcriber, or custom input method) is activated.

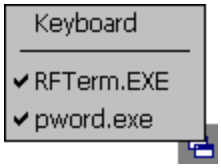
The check to the left of the application name indicates that the application is active.

If the application is listed but does not have a checkmark to the left of the application name, this means the application is configured in AppLock and can be manually launched by clicking on the application name in the list.

Using a Stylus Tap

When the mobile device enters end-user mode, a Switchpad icon (it looks like three tiny windows one above the other) is displayed in the lower right corner of the display. The Switchpad is always visible on top of the application in focus. However, if only one application is configured in AppLock and the Input Panel is disabled the Switchpad is not visible.

When the user taps the Switchpad icon, a menu is displayed showing the applications available to the user. The user can tap an application name in the popup menu and the selected application is brought to the foreground. The previous application continues to run in the background. Stylus taps affect the application in focus only. When the user needs to use the Input Panel, they tap the Keyboard option. Input Panel taps affect the application in focus only.



See Also: Application Panel > Launch > Manual (Launch) and Allow Close

Using the Switch Key Sequence

One switch key sequence (or hotkey) is defined by the administrator for the end-user to use when switching between locked applications. This is known as the **Activation key**. The Activation key is assigned by the Administrator using the Global Key parameter. When the switch key sequence is pressed on the keypad, the next application in the AppLock configuration is moved to the foreground and the previous application moves to the background. The previous application continues to run in the background. End-user key presses affect the application in focus only.

See Also: Start > Settings > Administration > Application Panel > Global Key

Hotkey (Activation hotkey)

The default Hotkey (Activation key) is **Ctrl+Spc**. The key sequence switches the focus between one application and another. Data entry affects the application running in the foreground only. Note that the system administrator may have assigned a different key sequence to use when switching applications.

Application Configuration

Settings > Control Panel > Administration icon

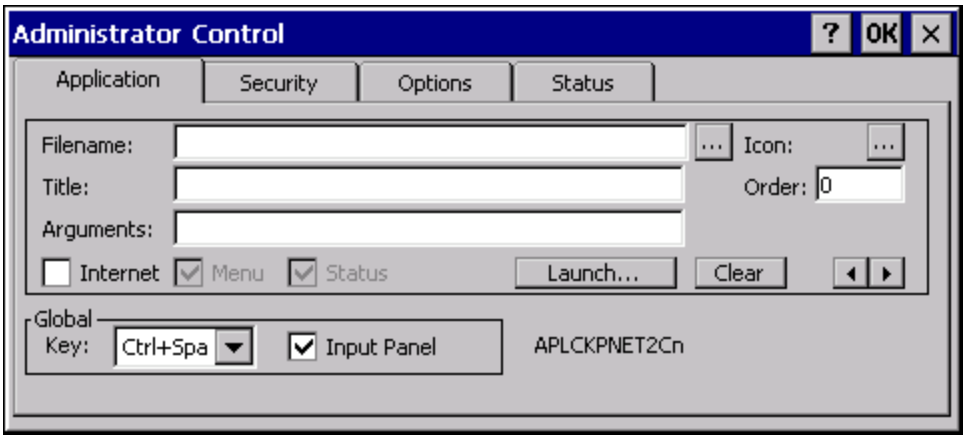
The default Administrator Hotkey sequence is **Shift+Ctrl+A**.

Administrator mode allows access to all features on the device. When the hotkey is pressed to switch into Administrator mode, a password prompt is displayed (if a password has been configured). A password must be entered within 30 seconds (and within three tries) or the password prompt is removed and the device remains in end-user mode with the focus returned to the locked application. Without entry of a valid password, the switch into Administrator mode will not occur.

The password prompt is displayed if a password has been configured. When the valid password is entered, the Administration Control panel is displayed. When a valid password is not entered within 30 seconds, the user is returned to the System Control Panel.

If a password has not been configured, the Administrator Control panel is displayed.

Application Panel



Use the Application tab options to select the applications to launch when the device boots up in End-user Mode.

If no application is specified when the Administrator Control Panel is closed, the mobile device reboots into Administrator mode. If a password has been set, but an application has not been specified, the user will be prompted for the password before entering administration mode. The password prompt remains on the display until a valid password is entered.

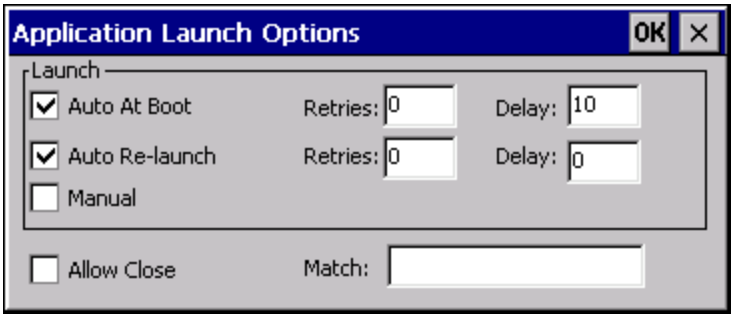
Option	Explanation
Filename	Default is blank. Move the cursor to the Filename text box and either type the application path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the application from the Browse dialog, tap OK.
Title	Default is blank. Enter the Title to be associated with the application. The assumption is that multiple copies of the same application may need unique titles in order to differentiate them in the Switchpad.
Arguments	Default is blank. Enter the command line parameters for the application in the Arguments text box.
Order	Default is 1. Enter the Order in which the application is to be loaded or presented to the end-user. Applications are launched in lowest to highest number order and do not need to be sequential.

Option	Explanation
Internet	Default is Disabled. Enable the Internet checkbox to use the End-user Internet Explorer (EUIE.EXE). When the checkbox is enabled, the Internet Menu and Internet Status are available. See the section titled End-user Internet Explorer (EUIE) for more details.
Launch Button	See following section titled Launch Button. *Note: AppLock Administrator Control panel file Launch option does not inter-relate with similarly-named options contained in other Control Panels.*
Global Key	Default is Ctrl+Spc. Select the Global Key key sequence the end-user is to press when switching between applications. The Global Key default key sequence must be defined by the AppLock Administrator. The Global key is presented to the end-user as the Activation key.
Global Delay	Default is 10 seconds. Enter the number of seconds that Applications must wait before starting to run after reboot. *Note: Delay (Global) may not be available in all versions of AppLock. You can simulate a Global Delay function by setting a delay for the first application (lowest Order) launched and setting the delay to 0 for all other applications. See Boot Options.*
Input Panel	Default is Disabled. Enable (check) to show the Keyboard option on the Switchpad menu. When enabled the input panel cannot be enabled or disabled for each individual application, and is available to the user for all configured applications.
Clear Button	Tap the Clear button to clear all currently displayed Filename or Application information. The Global settings are not cleared.
Scroll Buttons	Use the left and right scroll buttons to move from application setup screen to application setup screen. The left and right buttons update the information on the screen with the previous or next configured application respectively.

Launch Button

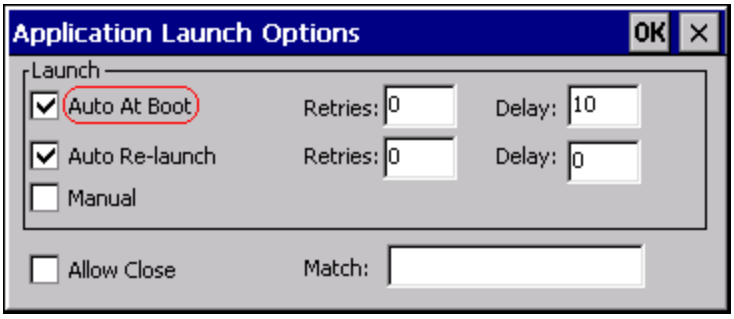
Note: The Launch button may not be available in all versions of Multi-AppLock. Contact Technical Assistance for assistance, downloads and AppLock update availability.

When clicked, displays the Launch options panel for the Filename selected on the Administration panel.



Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto At Boot



Default is Enabled.

Auto At Boot

When enabled, automatically launches (subject to the specified Delay in seconds) the application after the unit is rebooted. If a Delay in seconds is specified, AppLock waits for the specified period of time to expire before launching the application. The Delay default value is 10 seconds; valid values are between 0 “no delay” and a maximum of 999 seconds.

Retries

This is the number of times the application launch will be retried if a failure occurs when the application is automatically launched at bootup. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches. The default is 0 retries.

Delay

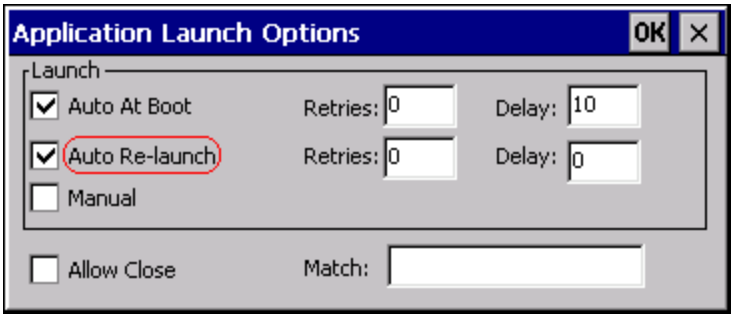
This timer is the time that AppLock waits prior to the initial launch of the selected application when it is automatically launched at bootup. Delay default is 10 seconds. Valid values are between 0 seconds (no delay) and 999 seconds.

The Auto At Boot delay is associated for each application; it will be either a value specified by the Administrator or it will be the delay default value. At startup, when a delay has been assigned for each application, AppLock waits for the delay associated with the first application to expire before launching the first application then AppLock waits for the delay associated with the second application to expire before launching the second application. AppLock continues in this manner until all applications are launched.

Note: A “Global Delay” can be accomplished by setting a timed delay for the first application to be launched (by lowest Order number) and no delay (0 seconds) for all other applications.

Note: Launch order is determined by the Order specified in the Application tab. The Order value does not have to be sequential.

Auto Re-Launch



Auto Re-Launch

Default is Enabled.

When enabled for a specific application, automatically re-launches it (subject to the specified Auto Re-Launch Delay in seconds) after it terminates. This option allows the Administrator to disable the re-launch operation. AppLock cannot prevent all applications from closing. When an application that AppLock cannot prevent from closing terminates, perhaps because of an error condition, AppLock re-launches the application when this option is enabled.

Note: If Allow Close is enabled and both Auto Re-launch and Manual (Launch) are disabled, the application cannot be restarted for the end-user or by the end-user after the application terminates.

Retries

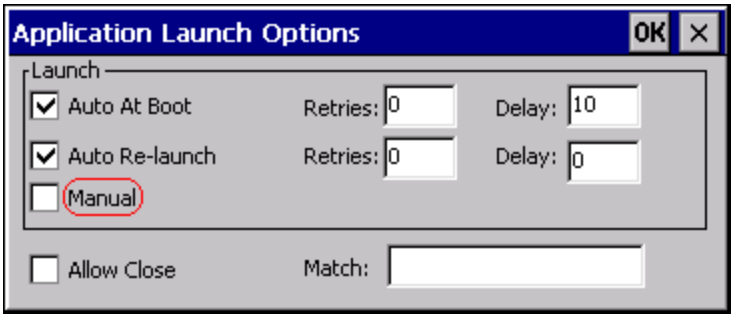
Default is 0 tries. Retries is the number of times AppLock will try to re-launch the application. The retry count is reset after an application is successfully launched and controlled by AppLock. Valid values are between 0 (no tries) and 99 tries or -1 for infinite. Infinite tries ends when the application successfully launches.

Delay

Default is 0 seconds (no delay). Delay is the amount of time AppLock waits prior to re-launching an application that has terminated. The delay is specified in seconds. Valid values are between 0 (no delay) and 99 seconds.

AppLock must also be configured to automatically re-launch an application. To AppLock, application termination by the end-user is indistinguishable from application termination for any other reason.

Manual (Launch)



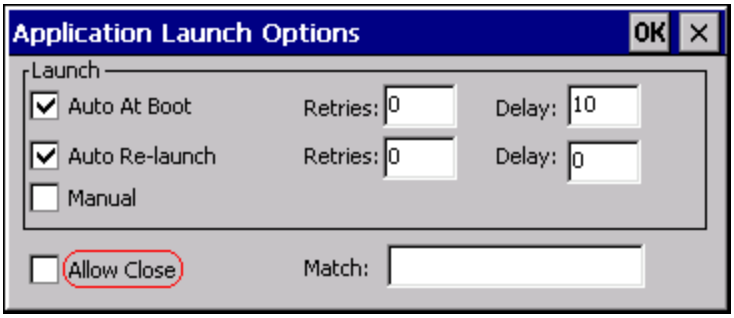
Default is Disabled. Enabling this option allows the end-user to launch the specified application(s). Upon bootup completion an application with Manual enabled is listed on the Switchpad accompanied by a checkmark that indicates the application is currently active or available for Launching. When an application name is tapped by the end-user, the application is launched (if inactive) and brought to the foreground.

Applications set up with Manual (Launch) enabled may or may not be launched at bootup. This function is based on the application's Auto At Boot setting. The applications have been listed as approved applications for end-user manual launch using the Switchpad menu structure. The approved applications are listed on the Switchpad. A checkmark indicates the applications active status.

When Manual (Launch) is disabled for an application, and Allow Close is enabled for the application, when the end-user closes the specific application it is no longer available (shown) on the Switchpad.

When Auto At Boot and Manual (Launch) are both disabled for a specific application, the application is 1) not placed on the list of approved applications for end-user manual launch and 2) never launched, and 3) not displayed on the Switchpad.

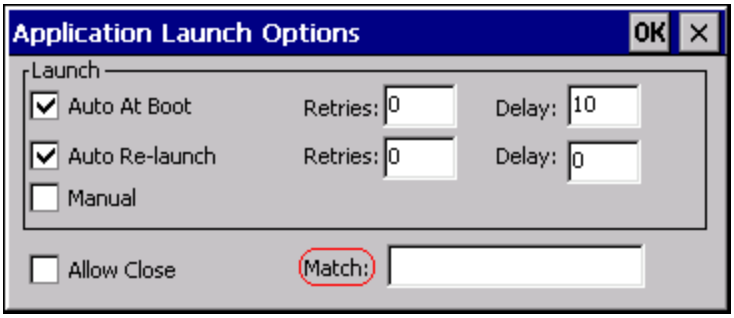
Allow Close



Default is Disabled. When enabled, the associated application can be closed by the end-user.

This option allows the administrator to configure applications that consume system resources to be terminated if an error condition occurs or at the end-user's request. Error conditions may generate a topmost popup requiring an end-user response, memory resource issues requiring an end-user response, etc. Also at the administrator's discretion, these types of applications can be started manually (see Manual [Launch]) by the end-user.

Match



Default is blank (match is not used).

AppLock works by associating display windows with the launched process ID. If an application uses different process IDs for windows it creates, the Match field must be used.

Use the Match field to specify up to 32 characters of the class name for the application.

For example:

- DOS applications using a standard DOS display box should specify **condev_appcls** in the Match textbox.
- Remote Desktop (remote.exe) should specify TSSHELLWND in the Match textbox.

Note: An update may be required to support locking remote.exe. Contact Technical Assistance for details.

End User Internet Explorer (EUIE)

AppLock supports applications that utilize Internet Explorer, such as .HTML pages and JAVA applications. The end user can run an application by entering the application name and path in Internet Explorer's address bar.

To prevent the end user from executing an application using this method, the address bar and Options settings dialog are restricted in Internet Explorer. This is accomplished by creating an Internet Explorer that is used in end user mode: End-user Internet Explorer (EUIE.EXE). The EUIE executes the Internet Explorer application in full screen mode which removes the address bar and status bar. The Options Dialog is also removed so the end user cannot re-enable the address bar.

The administrator specifies the EUIE by checking the Internet checkbox in the Application tab of the Administrator applet. The Internet application should then be entered in the Application text box.

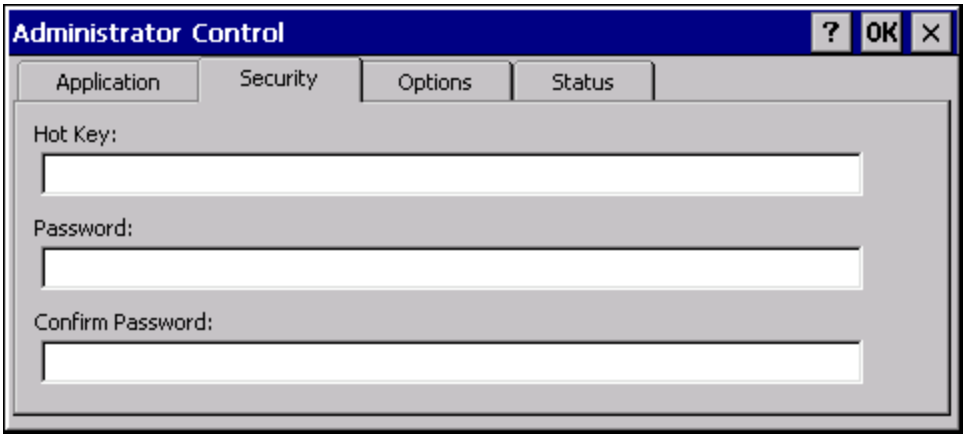
When the Internet checkbox is enabled, the Menu and Status check boxes are available.

Enabling the Menu checkbox displays the EUIE menu which contains navigation functions like Back, Forward, Home, Refresh, etc., functions that are familiar to most Internet Explorer users. When the Menu checkbox is blank, the EUIE menu is not displayed and Navigation functions are unavailable.

When the Status checkbox is enabled, the status bar displayed by EUIE gives feedback to the end-user when they are navigating the Internet.

If the standard Internet Explorer that is shipped with the mobile device is desired, it should be treated like any other application. This means that IEXPLORER.EXE should be specified in the Application text box and the Internet application should be entered in the command line. In this case, do not check the Internet checkbox.

Security Panel



Hotkey

Specify the hotkey sequence that triggers AppLock to switch between administrator and user modes and the password required to enter Administrator mode. The default hotkey sequence is **Shift+Ctrl+A**.

A 2nd key keypress is an invalid keypress for a hotkey sequence.

Move the cursor to the Hot Key text box. Enter the new hot key sequence by first pressing the Shift state key followed by a normal key. The hotkey selected must be a key sequence that the application being locked does not use. The hotkey sequence is intercepted by AppLock and is not passed to the application.

Input from the keyboard or Input Panel is accepted with the restriction that the normal key must be pressed from the keyboard when switching modes. The hotkey sequence is displayed in the Hot key text box with “Shift”, “Alt”, and “Ctrl” text strings representing the shift state keys. The normal keyboard key completes the hotkey sequence. The hotkey must be entered via the keypad. Some hotkeys cannot be entered via the Input Panel. Also, hotkeys entered via the SIP are not guaranteed to work properly when switching operational modes.

For example, if the ‘Ctrl’ key is pressed followed by ‘A’, “Ctrl+A” is entered in the text box. If another key is pressed after a normal key press, the hotkey sequence is cleared and a new hotkey sequence is started.

A normal key is required for the hotkey sequence and is unlike pressing the normal key during a mode switch; this key can be entered from the SIP when configuring the key. However, when the hotkey is pressed to switch modes, the normal key must be entered from the keypad; it cannot be entered from the SIP.

Password

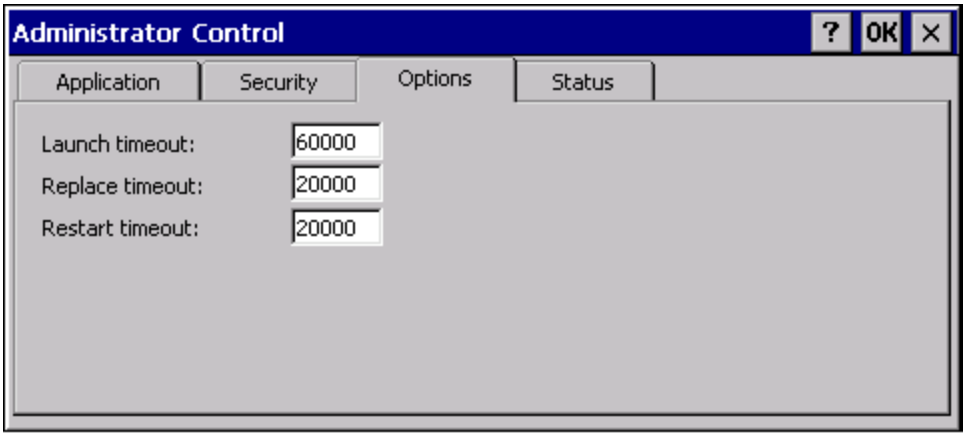
Move the cursor to the Password text box. The passwords entered in the Password and Confirm Password fields must match. Passwords are case sensitive.

When the user exits the Administrator Control panel, the two passwords are compared to verify that they match. If they do not match, a dialog box is displayed notifying the user of the error. After the user closes the dialog box, the Security Panel is displayed and the password can then be entered and confirmed again. If the passwords match, the password is encrypted and saved.

See Also: Passwords and AppLock Help

Options Panel

AppLock contains several types of delays and timeouts to accommodate different applications. Please note that the delays specified on the Launch panel are delays before AppLock attempts to start the specified application(s). The timeouts specified on this panel are delays after AppLock has attempted to launch the application.



Launch timeout

This timeout specifies the period of time for AppLock to wait for the application to initially launch after the application has been called. For example, if the application takes time to launch and then initialize before a display window is created, use this delay to specify the delay period.

Replace timeout

This timeout specifies the period of time for AppLock to wait after an initial screen (like a password prompt screen) is replaced by another application window.

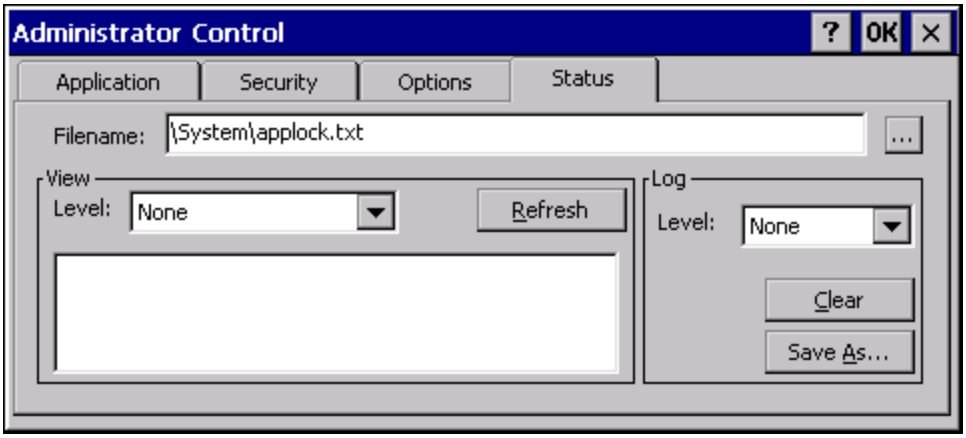
Restart timeout

This specifies the period of time for AppLock to wait for an application to restart. If the application fails to restart automatically, AppLock then proceeds according to the options selected when the application was configured on the Application and Launch panels.

Status Panel

Use the Status panel to view the log of previous AppLock operations and to configure which messages are to be recorded during AppLock operation.

Status information is stored in a specific location on the storage device and in a specific logfile specified by the Administrator. For this reason, the administrator can configure the type of status information that is logged, as well as clear the status information.



Move the cursor to the Filename text box and either type the logfile path or tap the Browse button (the … button). The standard Windows CE Browse dialog is displayed. After selecting the logfile from the Browse dialog, tap OK.

Note: If your Status Panel does not look like the figure shown above, you may have the Single Application version which does not have as many options.

View

Error	Error status messages are logged when an error occurs and is intended to be used by the administrator to determine why the specified application cannot be locked.
Process	Processing status shows the flow control of AppLock components and is mainly intended for Customer Service when helping users troubleshoot problems with their AppLock program.
Extended	Extended status provides more detailed information than that logged by Process Logging.
All	All messages are displayed.

Tap the Refresh button after changing from one view level to another. The filtered records are displayed, all others are not displayed.

Log

Note: If a level higher than Error is selected, the status should be cleared frequently by the administrator.

In addition to the three view levels the administrator can select that all status information be logged or turn off all status information logging completely. The system default is 'None'; however to reduce registry use, the administrator may want to select 'None' after verifying the configuration. Tap the Clear button to clear the status information from the registry.

- None
- Error
- Processing
- Extended
- All

Save As

When the 'Save As'… button is selected, a standard 'Save As' dialog screen is displayed. Specify the path and filename. If the filename exists, the user is prompted whether the file should be overwritten. If the file does not exist, it is created.

See Also: Error Messages

AppLock Help

The mobile device won't switch from Administration mode to end-user mode.

If the configuration is valid for one application but not the other, the switch to end-user mode fails. AppLock stays in Administration mode and is stopped until the Administrator password is entered.

The hotkey sequence needed is not allowed. What does this mean?

When the Administrator is selecting a hotkey sequence to use when switching user modes, they are not allowed to enter key combinations that are reserved by installed software applications. Only RFTerm key combinations are validated.

When RFTerm is installed on the mobile device and an RFTerm restricted key sequence is specified as a hotkey sequence by the Administrator, the following error message is displayed in a message box:

```
Selected hotkey is not allowed. Please reenter.
```

When RFTerm is not installed on the mobile device, the RFTerm keys are not restricted from use.

Can't locate the password that has been set by the administrator?

Contact Technical Assistance for information.

AppLock Error Messages

Any messages whose first word is an 'ing' word is output prior to the action described in the message. For example, "Switching to admin-hotkey press" is logged after the administrator has pressed the hotkey but prior to starting the switch process.

For all operations that can result in an error, an Error level message is displayed when a failure occurs. These messages contain the word "failure". These messages have a partner Extended level message that is logged which contains the word "OK" if the action completed successfully rather than with an error.

For processing level messages, "Enter…" is logged at the beginning of the function specified in the message and "Exit…" is logged at the end (just before the return) of the function specified in the message.

Message	Explanation and/or corrective action	Level
Error reading hotkey	The hotkey is read but not required by AppLock.	LOG_EX
Error reading hotkey; using default	A hotkey is required. If there is a failure reading the hotkey, the internal factory default is used.	LOG_ERROR
App Command Line= <Command line>	Command line of the application being locked	LOG_ PROCESSING
App= <Application name>	Name of the application being locked	LOG_ PROCESSING
dwProcessID= <#>	Device ID of the application being locked	LOG_EX
Encrypt exported key len <#>	Size of encrypt export key	LOG_EX
Encrypt password length= <#>	The length of the encrypted password.	LOG_EX
Encrypted data len <#>	Length of the encrypted password	LOG_EX
hProcess= <#>	Handle of the application being locked	LOG_EX
Key pressed = <#>	A key has been pressed and trapped by the hotkey processing.	LOG_EX

Message	Explanation and/or corrective action	Level
**********	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Address of keyboard hook procedure failure	AppLock found the kbdhook.dll, but was unable to get the address of the initialization procedure. For some reason the dll is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Address of keyboard hook procedure OK	AppLock successfully retrieved the address of the keyboard filter initialization procedure.	LOG_EX
Alt pressed	The Alt key has been pressed and trapped by the HotKey processing.	LOG_EX
Alt	Processing the hotkey and backdoor entry	LOG_EX
Application handle search failure	The application being locked did not complete initialization.	LOG_ERROR
Application handle search OK	The application initialized itself successfully	LOG_ERROR
Application load failure	The application could not be launched by AppLock; the application could not be found or is corrupted.	LOG_ERROR
Backdoor message received	The backdoor keys have been pressed. The backdoor hotkeys provide a method for customer service to get a user back into their system without editing the registry or reloading the device.	LOG_ PROCESSING
Cannot find kbdhook.dll	The load of the keyboard filter failed. This occurs when the dll is missing or is corrupted. Look in the \Windows directory for kbdhook.dll. If it exists, delete it. Also delete AppLock.exe from the \Windows directory and reboot the unit. Deleting AppLock.exe triggers the AppLock system to reload.	LOG_ERROR
Converted Pwd	Converted password from wide to mbs.	LOG_EX
Could not create event EVT_HOTKEYCHG	The keyboard filter uses this event at the Administrator Control panel. The event could not be created.	LOG_ERROR
Could not hook keyboard	If the keyboard cannot be controlled, AppLock cannot process the hotkey. This failure prevents a mode switch into user mode.	LOG_ERROR
Could not start thread HotKeyMon	The keyboard filter must watch for hot key changes. The watch process could not be initiated.	LOG_ERROR
Ctrl after L or X	Processing the backdoor entry.	LOG_EX
Ctrl pressed	The Ctrl key has been pressed and trapped by the HotKey processing.	LOG_EX
Ctrl	Processing the hotkey and backdoor entry.	LOG_EX
Decrypt acquire context failure	Unable to decrypt password.	LOG_ERROR
Decrypt acquired context OK	Decryption process ok.	LOG_EX
Decrypt create hash failure	Unable to decrypt password.	LOG_ERROR
Decrypt created hash OK	Decryption process ok.	LOG_EX
Decrypt failure	Unable to decrypt password.	LOG_ERROR
Decrypt import key failure	Unable to decrypt password.	LOG_ERROR
Decrypt imported key OK	Decryption process ok.	LOG_EX

Message	Explanation and/or corrective action	Level
Encrypt acquire context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquire encrypt context failure	Unable to encrypt password.	LOG_ERROR
Encrypt acquired encrypt context OK	Encrypt password process successful.	LOG_EX
Encrypt create hash failure	Unable to encrypt password.	LOG_ERROR
Encrypt create key failure	Unable to encrypt password.	LOG_ERROR
Encrypt created encrypt hash OK	Encrypt password process successful.	LOG_EX
Encrypt export key failure	Unable to encrypt password.	LOG_ERROR
Encrypt export key length failure	Unable to encrypt password.	LOG_ERROR
Encrypt exported key OK	Encrypt password process successful.	LOG_EX
Encrypt failure	The password encryption failed.	LOG_ERROR
Encrypt gen key failure	Unable to encrypt password.	LOG_ERROR
Encrypt generate key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key failure	Unable to encrypt password.	LOG_ERROR
Encrypt get user key ok	Encrypt password process successful.	LOG_EX
Encrypt hash data failure	Unable to encrypt password.	LOG_ERROR
Encrypt hash data from pwd OK	Encrypt password process successful.	LOG_EX
Encrypt length failure	Unable to encrypt password.	LOG_ERROR
Encrypt out of memory for key	Unable to encrypt password.	LOG_ERROR
Encrypted data OK	The password has been successfully encrypted.	LOG_EX
Enter AppLockEnumWindows	In order for AppLock to control the application being locked so it can prevent the application from exiting, AppLock launches the application and has to wait until it has created and initialized its main window. This message is logged when the function that waits for the application initialization is entered.	LOG_EX
Enter DecryptPwd	Entering the password decryption process.	LOG_ PROCESSING
Enter EncryptPwd	Entering the password encryption processing.	LOG_ PROCESSING
Enter FullScreenMode	Entering the function that switches the screen mode. In full screen mode, the taskbar is hidden and disabled.	LOG_ PROCESSING
Enter GetAppInfo	Processing is at the beginning of the function that retrieves the application information from the registry.	LOG_ PROCESSING
Enter password dialog	Entering the password dialog processing.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Enter password timeout	Entering the password timeout processing.	LOG_ PROCESSING
Enter restart app timer	Some application shut down before AppLock can stop it. In these cases, AppLock gets notification of the exit. When the notification is received, AppLock starts a timer to restart the application. This message logs that the timer has expired and the processing is at the beginning of the timer function.	LOG_ PROCESSING
Enter TaskbarScreenMode	Entering the function that switches the screen to non-full screen mode and enable the taskbar.	LOG_ PROCESSING
Enter ToAdmin	Entering the function that handles a mode switch into admin mode.	LOG_ PROCESSING
Enter ToUser	Entering the function that handles the mode switch to user mode	LOG_ PROCESSING
Enter verify password	Entering the password verification processing.	LOG_ PROCESSING
Exit AppLockEnumWindows-Found	There are two exit paths from the enumeration function. This message denotes the enumeration function found the application.	LOG_ PROCESSING
Exit AppLockEnumWindows-Not found	There are two exit paths from the enumeration function. This message denotes the enumeration function did not find the application.	LOG_ PROCESSING
Exit DecryptPwd	Exiting password decryption processing.	LOG_ PROCESSING
Exit EncryptPwd	Exiting password encryption processing.	LOG_ PROCESSING
Exit FullScreenMode	Exiting the function that switches the screen to full screen.	LOG_ PROCESSING
Exit GetAppInfo	Processing is at the end of the function that retrieved the application information from the registry.	LOG_ PROCESSING
Exit password dialog	Exiting password prompt processing.	LOG_ PROCESSING
Exit password dialog-cancel	Exiting password prompt w/cancel.	LOG_ PROCESSING
Exit password dialog-OK	Exiting password prompt successfully.	LOG_ PROCESSING
Exit password timeout	Exiting password timeout processing.	LOG_ PROCESSING
Exit restart app timer	Processing is at the end of the timer function	LOG_ PROCESSING
Exit TaskbarScreenMode	Exiting the function that switches the screen mode back to normal operation for the administrator.	LOG_ PROCESSING
Exit ToAdmin	Exiting the function that handles the mode switch into admin mode.	LOG_ PROCESSING
Exit ToUser	Exiting the user mode switch function.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Exit ToUser-Registry read failure	The AppName value does not exist in the registry so user mode cannot be entered.	LOG_ PROCESSING
Exit verify password-no pwd set	Exiting password verification.	LOG_ PROCESSING
Exit verify password-response from dialog	Exiting password verification.	LOG_ PROCESSING
Found taskbar	The handle to the taskbar has been found so that AppLock can disable it in user mode.	LOG_ PROCESSING
Getting address of keyboard hook init procedure	AppLock is retrieving the address of the keyboard hook.	LOG_ PROCESSING
Getting configuration from registry	The AppLock configuration is being read from the registry. This occurs at initialization and also at entry into user mode. The registry must be re-read at entry into user mode in case the administration changed the settings of the application being controlled.	LOG_ PROCESSING
Getting encrypt pwd length	The length of the encrypted password is being calculated.	LOG_EX
Hook wndproc failure	AppLock is unable to lock the application. This could happen if the application being locked encountered an error after performing its initialization and shut itself down prior to being locked by AppLock.	LOG_ERROR
Hook wndproc of open app failure	The application is open, but AppLock cannot lock it.	LOG_ERROR
Hot key event creation failure	The Admin applet is unable to create the hotkey notification.	LOG_ERROR
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key pressed	Processing the hotkey and backdoor entry	LOG_EX
Hot key set event failure	When the administrator changes the hotkey configuration the hotkey controller must be notified. This notification failed.	LOG_ERROR
Hotkey press message received	The user just pressed the configured hotkey.	LOG_ PROCESSING
In app hook:WM_SIZE	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window size and corrects it.	LOG_EX
In app hook:WM_ WINDOWPOSCHANGED	In addition to preventing the locked application from exiting, AppLock must also prevent the application from enabling the taskbar and resizing the application's window. This message traps a change in the window position and corrects it.	LOG_EX
Initializing keyboard hook procedure	AppLock is calling the keyboard hook initialization.	LOG_ PROCESSING
Keyboard hook initialization failure	The keyboard filter initialization failed.	LOG_ERROR
Keyboard hook loaded OK	The keyboard hook dll exists and loaded successfully.	LOG_EX
L after Ctrl	Processing the backdoor entry.	LOG_EX
Loading keyboard hook	When AppLock first loads, it loads a dll that contains the keyboard hook processing. This message is logged prior to the load attempt.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Open failure	The status information is being saved to a file and the file open has failed. This could occur if the file is write protected. If the file does not exist, it is created.	LOG_ERROR
Open registry failure	If the Administration registry key does not exist, the switch to user mode fails because the AppName value in the Administration key is not available.	LOG_ERROR
Opened status file	The status information is being saved to a file and the file has been opened successfully.	LOG_EX
Out of memory for encrypted pwd	Not enough memory to encrypt the password.	LOG_ERROR
pRealTaskbarWndProc already set	The taskbar control has already been installed.	LOG_EX
Pwd cancelled or invalid-remain in user mode	The password prompt was cancelled by the user or the maximum number of failed attempts to enter a password was exceeded.	LOG_EX
Read registry error-hot key	The hotkey registry entry is missing or empty. This is not considered an error. The keyboard hook uses an embedded default if the value is not set in the registry.	LOG_ERROR
Read registry failure-app name	AppName registry value does not exist or is empty. This constitutes a failure for switching into user mode.	LOG_ERROR
Read registry failure-Cmd Line	AppCommandLine registry entry is missing or empty. This is not considered an error since command line information is not necessary to launch and lock the application.	LOG_ERROR
Read registry failure-Internet	The Internet registry entry is missing or empty. This is not considered an error since the Internet value is not necessary to launch and lock the application.	LOG_ERROR
Registering Backdoor MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both AppLock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING
Registering Hotkey MSG	The AppLock system communicates with the keyboard hook via a user defined message. Both Applock.exe and Kbdhook.dll register the message at initialization.	LOG_ PROCESSING
Registry read failure at reenter user mode	The registry has to be read when entering user mode is the AppName is missing. This user mode entry is attempted at boot and after a hotkey switch when the administrator has closed the application being locked or has changed the application name or command line.	LOG_ERROR
Registry read failure at reenter user mode	The registry has to be read when switching into user mode. This is because the administrator can change the settings during administration mode. The read of the registry failed which means the Administration key was not found or the AppName value was missing or empty.	LOG_ERROR
Registry read failure	The registry read failed. The registry information read when this message is logged is the application information. It the Administration key cannot be opened or if the AppName value is missing or empty, this error is logged. The other application information is not required. If the AppName value is not available, AppLock cannot switch into user mode.	LOG_ERROR
Reset system work area failure	The system work area is adjusted when in user mode to cover the taskbar area. The system work area has to be adjusted to exclude the taskbar area in administration mode. AppLock was unable to adjust this area.	LOG_ERROR
Shift pressed	The Shift key has been pressed and trapped by the HotKey processing.	LOG_EX
Shift	Processing the hotkey and backdoor entry	LOG_EX
Show taskbar	The taskbar is now being made visible and enabled.	LOG_ PROCESSING

Message	Explanation and/or corrective action	Level
Switching to admin-backdoor	The system is currently in user mode and is now switching to admin mode. The switch occurred because of the backdoor key presses were entered by the administrator.	LOG_ PROCESSING
Switching to admin-hotkey press	The system is currently in user mode and is now switching to admin mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Switching to admin-kbdhook.dll not found	The keyboard hook load failed, so AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-keyboard hook initialization failure	If the keyboard hook initialization fails, AppLock switches to admin mode. If a password is specified, the password prompt is displayed and remains until a valid password is entered.	LOG_ PROCESSING
Switching to admin-registry read failure	See the explanation of the “Registry read failure” above. AppLock is switching into Admin mode. If a password has been configured, the prompt will be displayed and will not be dismissed until a valid password is entered.	LOG_ PROCESSING
Switching to TaskbarScreenMode	In administration mode, the taskbar is visible and enabled.	LOG_EX
Switching to user mode	The registry was successfully read and AppLock is starting the process to switch to user mode.	LOG_ PROCESSING
Switching to user-hotkey press	The system is currently in admin mode and is now switching to user mode. The switch occurred because of a hotkey press by the administrator.	LOG_ PROCESSING
Taskbar hook failure	AppLock is unable to control the taskbar to prevent the locked application from re-enabling it.	LOG_ERROR
Taskbar hook OK	AppLock successfully installed control of the taskbar.	LOG_EX
Timeout looking for app window	After the application is launched, AppLock must wait until the application has initialized itself before proceeding. The application did not start successfully and AppLock has timed out.	LOG_ERROR
ToUser after admin, not at boot	The user mode switch is attempted when the device boots and after the administrator presses the hotkey. The mode switch is being attempted after a hotkey press.	LOG_EX
ToUser after admin-app still open	The switch to user mode is being made via a hotkey press and the administrator has left the application open and has not made any changes in the configuration.	LOG_EX
ToUser after admin-no app or cmd line change	If user mode is being entered via a hotkey press, the administrator may have left the configured application open. If so, AppLock does not launch the application again unless a new application or command line has been specified; otherwise, it just locks it.	LOG_EX
Unable to move desktop	The desktop is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unable to move taskbar	The taskbar is moved when switching into user mode. This prevents them from being visible if the application is exited and restarted by the timer. This error does not affect the screen mode switch; processing continues.	LOG_ERROR
Unhook taskbar wndproc failure	AppLock could not remove its control of the taskbar. This error does not affect AppLock processing	LOG_ERROR
Unhook wndproc failure	AppLock could not remove the hook that allows monitoring of the application.	LOG_ERROR
Unhooking taskbar	In administration mode, the taskbar should return to normal operation, so AppLock’s control of the taskbar should be removed.	LOG_EX

Message	Explanation and/or corrective action	Level
Unhooking wndproc	When the administrator leaves user mode, the device is fully operational; therefore, AppLock must stop monitoring the locked application.	LOG_EX
WM_SIZE adjusted	This message denotes that AppLock has readjusted the window size.	LOG_EX
X after Ctrl+L	Processing the backdoor entry.	LOG_EX
Ret from password <#>	Return value from password dialog.	LOG_EX
Decrypt data len <#>	Length of decrypted password.	LOG_EX
Window handle to enumwindows=%x	The window handle that is passed to the enumeration function. This message can be used by engineering with other development tools to trouble shoot application lock failures.	LOG_EX
WM_WINDOWPOSCHG adjusted=%x	Output the window size after it has been adjusted by AppLock	LOG_EX

Bluetooth

Start > Settings > Control Panel > Bluetooth

Note: Contact Technical Assistance for upgrade availability if your Bluetooth control panel is not the same as the control panels presented in this section.

Discover and manage pairing with nearby Bluetooth devices.

Factory Default Settings

Discovered Devices	None
Settings	
Turn Off Bluetooth	Disabled
Computer is connectable	Enabled
Computer is discoverable	Disabled
Prompt if devices request to pair	Enabled
Continuous search	Disabled
Filtered Mode	Enabled
Printer Port on COM 9:	Disabled (unchecked) by default in both Filtered and Non Filtered Modes. The option is dimmed in Non Filtered Mode.
Logging	Disabled
Computer Friendly Name	System Device Name
Reconnect	
Report lost connection	Enabled
Report when reconnected	Disabled
Report failure to reconnect	Enabled
Clear Pairing Table on boot	Disabled
Auto Reconnect on Boot	Enabled
Auto Reconnect	Enabled
OPP Setup	
Inbox	\My Device\My Documents\DefaultInbox
Outbox	\My Device\My Documents\DefaultOutbox
Write Capable	Enabled
Enable Notifications	Enabled
Disable LXEZ Pairing OPP	Unchecked, OPP is enabled

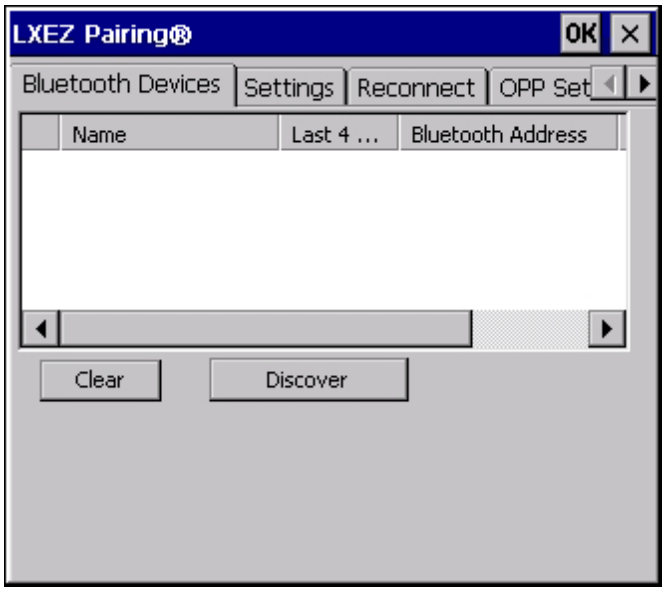
Bluetooth taskbar Icon state and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. There may be audible or visual signals as paired devices re-connect with the VX7.

- The default Bluetooth setting is On.
- The VX7 cannot be discovered by other Bluetooth devices when the **Computer is discoverable** option is disabled (unchecked) on the Settings panel.
- Other Bluetooth devices cannot be discovered if they have been set up to be Non-Discoverable or Invisible.
- When **Filtered Mode** is enabled, the VX7 can pair with one Bluetooth scanner and one Bluetooth printer.
- When **Filtered Mode** is disabled, the VX7 can pair with up to four Bluetooth devices, with a limit of one scanner, one printer, two HID[1] devices (one Mouse, one Keyboard), one PAN[2] device, and one DUN[3] device connected at the same time.
- It is not necessary to disconnect a paired scanner and printer before a different scanner or printer is paired with the VX7.
- The target Bluetooth device should be as close as possible (up to 32.8 ft (10 meters) Line of Sight) to the VX7 during the pairing process.

Assumption: The System Administrator has Discovered and Paired targeted Bluetooth devices for the VX7. The VX7 operating system has been upgraded to the revision level required for Bluetooth client operation. An application (or API) is available that will accept data from serial Bluetooth devices.

Bluetooth Devices

The Bluetooth Devices tab displays any device previously discovered and paired with the VX7.



[1]Human Interface Device profiles used by Bluetooth keyboards, mice, pointing devices and remote monitoring devices.
[2]Personal Area Networking profile. Un-modified Ethernet payloads (using BNEP) can exchange packets between Bluetooth devices. PANU is a PAN User service that uses either the NAP or the GN service.
[3]Dial-Up Networking provides access to the Internet and other dial-up services using Bluetooth technology.

Discover

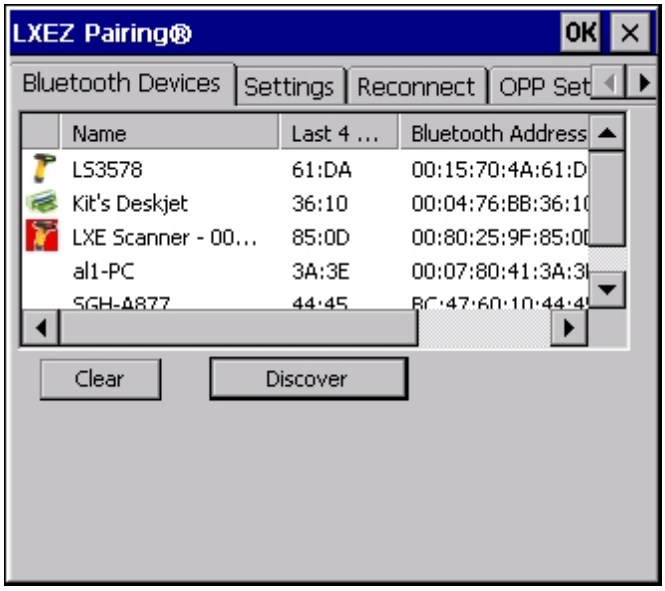
Tap the Discover button to locate all discoverable Bluetooth devices in the vicinity. The Discovery process also queries for the unique identifier of each device discovered.

Stop Button

Tap Stop at any time to end the Discover and Query for Unique Identifier functions. Devices not paired are not shown after any reboot sequence.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the VX7 Bluetooth scanning range, the Bluetooth connection between the paired device and the VX7 is lost. There may be audible or visual signals as paired devices disconnect from the VX7.

Bluetooth Device List



The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Scanner or a Printer. The Bluetooth panel assigns an icon to the device name.

The discovered paired devices may or may not be identified with an icon. Discovered devices without an icon can be paired as a Serial device, a Bluetooth scanner, a Bluetooth printer, a PAN, and a DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. The Bluetooth panel assigns an icon to the device name.

An icon with a red background indicates the device's Bluetooth connection is inactive.

An icon with a white background indicates the device is connected to the VX7 and the device's Bluetooth connection is active.

Double-tap a device in the list to open the device properties menu. The target device does not need to be active.

Clear Button

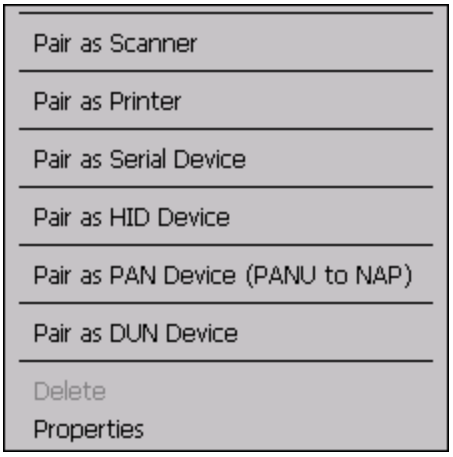
Deletes all devices from the Device table that are not currently paired. A dialog box is presented, "Delete all disconnected devices? Yes/No". Tap the Yes button to remove disconnected or deleted devices from the device table. The devices are removed from the Device table after any reboot sequence or after closing and reopening the Bluetooth panels. Tap the No button to make no changes. See Clear Pairing Table on Boot.

Bluetooth Device Menu

Pre-requisite: The Discover button has been clicked and there are Bluetooth devices listed.

Click on a device in the list to highlight it. Double click the highlighted device to display the Bluetooth Device right click menu. The Bluetooth device does not need to be active.

Filtered Mode Enabled

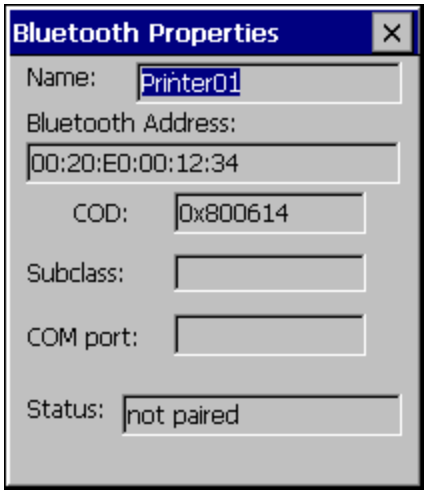


Filtered Mode Disabled

Right Click Menu Options

Pair as Scanner	Receive data from the highlighted Bluetooth scanner or Bluetooth imager.
Pair as Printer	Send data to the highlighted Bluetooth printer.
Pair as Serial Device	Communicate with the highlighted serial Bluetooth device. This option is available when Filtered Mode is disabled.
Pair as HID Device	Communicate with the highlighted HID (Human Interface Device). This option is available when Filtered Mode is disabled/unchecked.
Pair as PAN Device (PANU to NAP)	Communicate with the highlighted PAN (Personal Area Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Pair as DUN Device	Communicate with the highlighted DUN (Dial-Up Networking) device. This option is available when Filtered Mode is disabled/unchecked.
Disconnect	Stop the connection between the VX7 and the highlighted paired Bluetooth device.
Delete	Remove an unpaired device from the Bluetooth device list. The highlighted device name and identifier is removed from the VX7 Bluetooth Devices panel after the user taps OK.
Properties	More information on the highlighted Bluetooth device.

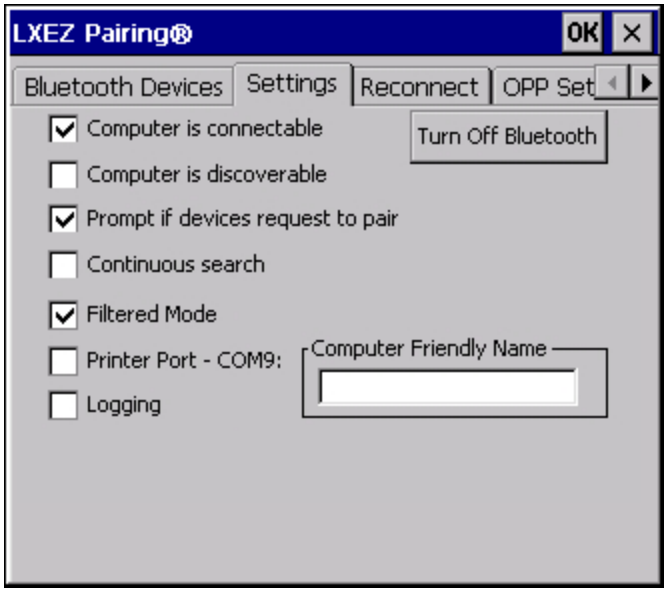
Bluetooth Device Properties



Data on the Bluetooth Properties panel cannot be changed by the user. The data displayed is the result of the device Query performed during the Discovery process.

The Status dialog box reflects the current state of the highlighted device.

Settings



Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

Turn Off Bluetooth

Tap the button to toggle the Bluetooth client On or Off. The button title changes from *Turn Off Bluetooth* to *Turn On Bluetooth*. When the button is dimmed (grey), the Bluetooth client cannot be disabled.

Default

The default value is Bluetooth On.

Options

Option	Function
Computer is connectable	This option is Enabled by default. Disable this option to inhibit VX7 connection initiated by a Bluetooth scanner.
Computer is discoverable	This option is Disabled by default. Enable this option to ensure other devices can discover the VX7.
Prompt if devices request to pair	This option is Enabled by default. A dialog box appears on the VX7 screen notifying the user a Bluetooth device requests to pair with the VX7. The requesting Bluetooth device does not need to have been Discovered by the VX7 before the pairing request is received. Tap the Accept button or the Decline button to remove the dialog box from the screen. *Note: In some cases, if a Bluetooth device is already paired this setting cannot be changed. If this is the case, an error message is displayed and the option is not changed. The Bluetooth device must be disconnected before changing this setting.*
Continuous Search	This option is Disabled by default. When enabled, the Bluetooth connection never stops searching for a device it has paired with when the connection is broken (such as the paired device entering Suspend mode, going out of range or being turned off). When disabled, after being enabled, the VX7 stops searching after 30 minutes. This option draws power from the Main Battery.
Filtered Mode	This option is Enabled by default. Determines whether the Bluetooth client discovers and displays all serial Bluetooth devices in the vicinity (Filtered Mode is disabled/unchecked) or the discovery result displays Bluetooth scanners and printers only (Filtered Mode is enabled/checked). When Filtered Mode is disabled, the VX7 can pair with up to four Bluetooth devices, with a limit of one Bluetooth scanner, one Bluetooth printer, one PAN, and one DUN connected at the same time. More than one HID device can be connected but only one Bluetooth mouse and one Bluetooth keyboard. A Warmboot is required every time Filtered Mode is toggled on and off.
Printer Port - COM9	This option is Disabled by default. This option assigns Bluetooth printer connection to COM9 instead of COM19. To enable this option, Filtered Mode must be enabled.
Logging	This option is Disabled by default. When logging is enabled, the VX7 creates *bt_log.txt* and stores it in the /System folder. Bluetooth activity logging is added to the text file as activity progresses. A *bt_log_bak.txt* file contains the data stored by *bt_log.txt* prior to reboot. During a reboot process, the VX7 renames *bt_log.txt* to *bt_log_bak.txt*. If a file already exists with that name, the existing file is deleted, the new *bt_log_bak.txt* file is added and a new *bt_log.txt* is created.
Computer Friendly Name	Default: Computer System Name (**System Panel > Device Name** tab). The name, or identifier, entered in **this** space by the System Administrator is used exclusively by Bluetooth devices and during Bluetooth communication.

Reconnect

Note: These options can still be checked or unchecked whether Bluetooth connection is enabled or disabled.

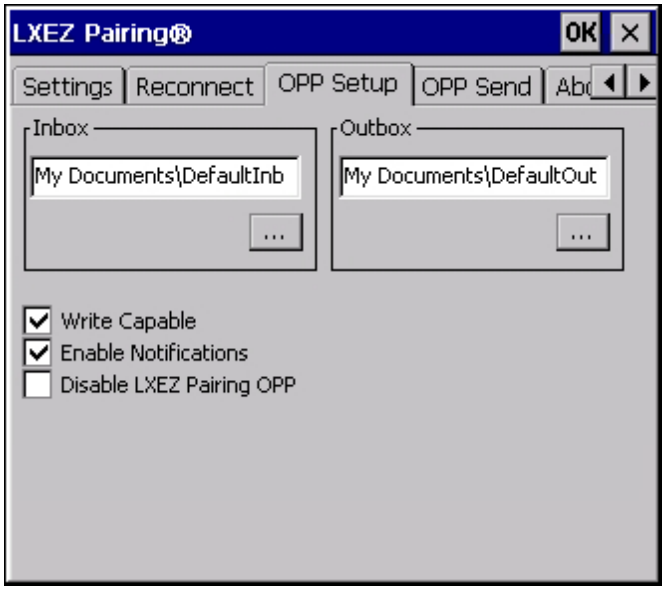
Options

Option	Function
Report when connection lost	This option is Enabled (checked) by default. There may be an audio or visual signal when a connection between a paired, active device is lost. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has stopped. Tap the ok button to remove the dialog box from the screen.
Report when reconnected	This option is Disabled (unchecked) by default. There may be an audio or visual signal when a connection between a paired, active device is made. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the paired Bluetooth devices has resumed. Tap the ok button to remove the dialog box from the screen.
Report failure to reconnect	This option is Enabled (checked) by default. The default time delay is 30 minutes. This value cannot be changed by the user. There may be an audio or visual signal when a connection between a paired, active device fails to re-connect. A visual signal may be a dialog box placed on the display notifying the user the connection between one (or all) of the previously paired Bluetooth devices has failed. Tap the X button or ok button to close the dialog box. Possible reasons for failure to reconnect: Timeout expired without reconnecting; attempted to pair with a device that is currently paired with another device; attempted to pair with a known device that moved out of range or was turned off; attempted to pair with a known device but the reason why reconnect failed is unknown.
Clear Pairing Table on Boot	This option is Disabled (unchecked) by default. When enabled (checked), all previous paired information is deleted upon any reboot sequence and no devices are reconnected. When enabled (checked) "Auto Reconnect on Boot" is automatically disabled (dimmed).
Auto Reconnect on Boot	This option is Enabled (checked) by default. All previously paired devices are reconnected upon any reboot sequence. When disabled (unchecked), no devices are reconnected upon any reboot sequence.

Option	Function
Auto Reconnect	This option is Enabled (checked) by default. This option controls the overall mobile Bluetooth device reconnect behavior. • When Auto Reconnect is disabled (unchecked), *Auto Reconnect on Boot* is automatically disabled and dimmed. • When Auto Reconnect is disabled (unchecked), no devices are reconnected in any situation. The status of *Auto Reconnect on Boot* is ignored and no devices are reconnected on boot. The status of *Clear Pairing Table on Boot* controls whether the pairing table is populated on boot. • When Auto Reconnect is enabled (checked) and *Auto Reconnect on Boot* is disabled (unchecked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). • When Auto Reconnect is enabled (checked) and *Clear Pairing Table on Boot* is enabled (checked), devices are not reconnected on boot, but are reconnected in other situations (example: return from out-of-range). The pairing table is cleared on boot. The status of *Auto Reconnect on Boot* is ignored and the option is automatically disabled (unchecked) and dimmed.

OPP Setup

Use this screen to setup the VX7 for Object Push Protocol (OPP).

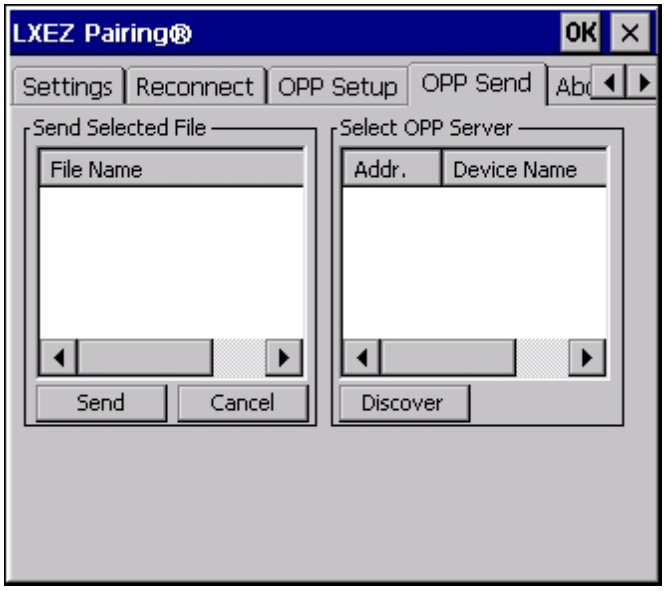


Option	Information
Inbox	This is an alphanumeric field displaying the currently selected Inbox. • The Inbox is the location where files pushed to the VX7 from a remote client are stored. Use the browse button **...** to browse to and select the Inbox folder. • Use Windows Explorer to create a custom directory, if desired, before selecting the Inbox folder. • The default Inbox is \My Device\My Documents\DefaultInbox.
Outbox	This is an alphanumeric field displaying the currently selected Outbox. • The Outbox is the location where files are stored to be pushed from the VX7 to a remote server. Use the browse button **...** to browse to and select the Outbox folder. • Use Windows Explorer to create a custom directory, if desired, before selecting the Outbox folder. The default Inbox is \My Device\My Documents\DefaultOutbox.
Write Capable	When checked, files may be written to the VX7. When unchecked, inbound files are rejected. This option is enabled (checked) by default.
Enable Notifications	When checked, the user is notified and may be prompted for a response when files are received by the VX7. When unchecked, inbound files are received with no notification to and no required action from the user. This option is enabled (checked) by default.

Option	Information
Disable LXEZ Pairing OPP	When checked, OPP is disabled in LXEZ Pairing. When unchecked, OPP is enabled in LXEZ Pairing. The default is unchecked, OPP is enabled for LXEZ Pairing. • Because only one application can use OPP at a given time, custom applications should disable OPP in LXEZ Pairing via an API call while the application is using OPP and restore this setting upon completion. • When this item is checked, the other parameter settings on this screen are unavailable (dimmed).

See Also: "Using OPP"

OPP Send



If LXEZ Pairing OPP is disabled, no file names or OPP servers are displayed on this tab. These areas are grayed out. Similarly the buttons on this tab are also inactive when LXEZ Pairing OPP is disabled.

Option	Information
Send Selected File From Outbox	This area displays the file listing from the currently selected Outbox. All files are shown (*.*). The most recently pushed file is highlighted, assuming that file is still present in the Outbox.
Select OPP Server from Remote Device List	This list displays the known OPP capable servers that the VX7 has previously discovered. The most recently paired server is selected and highlighted.

Buttons

Send - Tapping this button sends (pushes) the selected file to the remote (server) device.

Cancel - Tapping this button cancels the send process initiated by tapping the **Send** button.

Discover - Tapping this button initiates a discovery of OPP devices. Results of the discovery are shown in the OPP Server selection box.

See Also: "Using OPP"

About

This panel lists the assigned Computer Friendly Name (that other devices may discover during their Discovery and Query process), the Bluetooth MAC address, and software version levels. The data cannot be edited by the user.

Using Bluetooth

Start > Settings > Control Panel > Bluetooth or Bluetooth icon in taskbar or Bluetooth icon on desktop

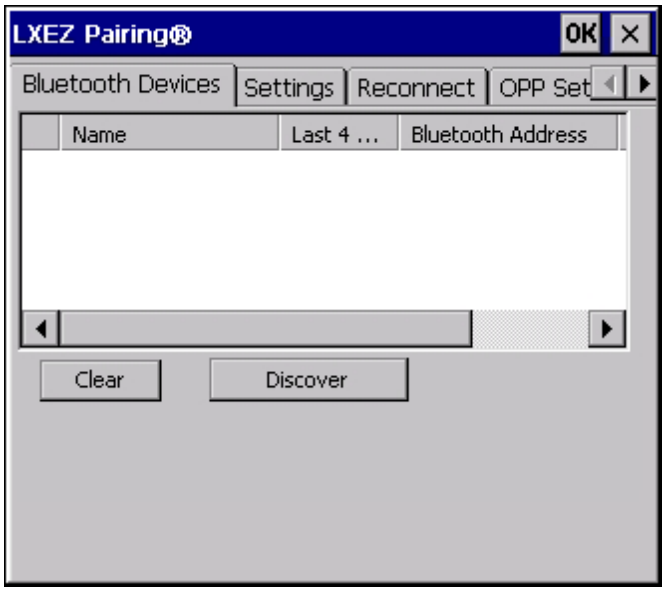
Bluetooth taskbar icon

The VX7 default Bluetooth setting is Enabled.

The VX7 Bluetooth® module is designed to Discover and pair with nearby Bluetooth devices.

Prerequisite: The Bluetooth devices have been setup to allow them to be "Discovered" and "Connected/Paired". The System Administrator is familiar with the pairing function of the Bluetooth devices.

Bluetooth Devices Display - Before Discovering Devices



*Note: When **Filtered Mode** is enabled, only certain Bluetooth printers or Bluetooth scanners/imagers are recognized and displayed in the Bluetooth panel. All other Bluetooth devices are ignored.*

Initial Configuration

1. Select **Start > Settings > Control Panel > Bluetooth** or tap the Bluetooth icon in the taskbar or on the desktop.
2. Tap the **Settings** Tab.
3. Change the **Computer Friendly Name** at the bottom of the Settings display. The Bluetooth VX7 default name is determined by the factory installed software version. Honeywell strongly urges assigning every VX7 a unique name (up to 32 characters) before Bluetooth Discovery is initiated.
4. Check or uncheck the VX7 Bluetooth options on the **Settings** and **Reconnect** tabs.
5. Tap the OK button to save your changes or the X button to discard any changes.

Subsequent Use

Note: Taskbar and Bluetooth device Icon states change as Bluetooth devices are discovered, paired, connected and disconnected. A taskbar Bluetooth icon with a red background indicates Bluetooth is active and not paired with any device. A device icon with a red background indicates a disconnected paired device.

1. Tap the **Bluetooth icon** in the taskbar or on the desktop to open the Bluetooth LXEZ Pairing application.
2. Tap the Bluetooth **Devices** tab.
3. Tap the **Discover** button. When the Bluetooth module begins searching for in-range Bluetooth devices, the button name changes to Stop. Tap the Stop button to cancel the Discover function at any time.
4. The discovered devices are listed in the Bluetooth **Devices** window.
5. **Highlight** a Bluetooth device in the Discovered window and double-tap to open the device properties menu.
6. Tap **Pair as Scanner** to set up the VX7 to receive scanner data.
7. Tap **Pair as Printer** to set up the VX7 to send data to the printer.
8. Tap **Serial Device** (when Filtered mode is disabled) to set up the VX7 to communicate with a Bluetooth serial device.
9. Tap HID Device to pair a HID device.
10. Tap PAN Device to pair a PAN device.
11. Tap DUN Device to pair a DUN device.
12. Tap **Disconnect** to stop pairing with the device. Once disconnected, tap **Delete** to remove the device name and data from the VX7 Bluetooth Devices list. The device is deleted from the list after the OK button is clicked.
13. Upon successful pairing, the selected device may react to indicate a successful connection. The reaction may be an audio signal from the device, flashing LED on the device, or a dialog box is placed on the VX7 display.
14. Whenever the VX7 is turned On, all previously paired, live, Bluetooth devices in the vicinity are paired, one at a time, with the VX7. If the devices cannot connect to the VX7 before the re-connect timeout time period expires (default is approximately 20 seconds for each paired device) there is no indication of the continuing disconnect state if Report Failure to Reconnect is disabled.

Bluetooth Indicators

The Bluetooth taskbar Icon state changes as Bluetooth devices are discovered, paired, connected and disconnected.

There may be audible or visual signals as paired devices re-connect with the VX7.

Taskbar Icon	Legend
	VX7 is connected to one or more of the targeted Bluetooth device(s).
	VX7 is not connected to any Bluetooth device. VX7 is ready to connect with any Bluetooth device. VX7 is out of range of all paired Bluetooth device(s). Connection is inactive.

Note: When an active paired device enters Suspend Mode, is turned Off or leaves the VX7 Bluetooth scan range, the Bluetooth connection between the paired device and the VX7 is lost. There may be audible or visual signals as paired devices disconnect from the VX7.

AppLock, if installed, does not stop the end-user from using Bluetooth applications, nor does it stop authorized Bluetooth-enabled devices from pairing with the VX7 while AppLock is in control.

Bluetooth Barcode Reader Setup

Please refer to the Bluetooth scanner manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance for Bluetooth product assistance.

Honeywell supports several different types of barcode readers. This section describes the interaction and setup for a mobile Bluetooth laser scanner or laser imager connected to the VX7 using Bluetooth functions.

Prerequisites

- The VX7 has the Bluetooth hardware and software installed. An operating system upgrade may be required. Contact Technical Assistance for details.
- If the VX7 has a Bluetooth address identifier barcode label affixed, then Bluetooth hardware and software is installed.
- The mobile Bluetooth laser scanner / laser imager battery is fully charged.
- The VX7 is connected to AC or DC (vehicle) power.
- *The barcode numbering examples in this segment are not real and should not be created nor scanned with a Bluetooth scanner.*
- To open the LXEZ Pairing program, tap **Start > Settings > Control Panel > Bluetooth** or tap the Bluetooth icon on the desktop or tap the Bluetooth icon in the taskbar.

Locate the barcode label, similar to the one shown above, attached to the VX7. The label is the Bluetooth address identifier for the VX7.

The mobile Bluetooth scanner / imager requires this information before discovering, pairing, connecting or disconnecting can occur.

The VX7 Bluetooth address identifier label should remain protected from damage (rips, tears, spills, soiling, erasure, etc.) at all times. It may be required when pairing, connecting, and disconnecting new Bluetooth barcode readers.

VX7 with Label

If the VX7 has a Bluetooth address barcode label attached, follow these steps:

1. Scan the Bluetooth address barcode label, attached to the VX7, with the Bluetooth mobile scanner.
2. If this is the first time the Bluetooth mobile scanner has scanned the VX7 Bluetooth label, the devices are paired. See section titled "Bluetooth Beep and LED Indications". If the devices do not pair successfully, go to the next step.
3. Open the LXEZ Pairing panel (**Start > Settings > Control Panel > Bluetooth**).
4. Tap **Discover.** Locate the Bluetooth scanner in the Discovery panel.
5. Double-tap the stylus on the Bluetooth **mobile device** in the list. The right-mouse-click menu appears.
6. Select **Pair as Scanner** to pair the VX7 with the Bluetooth mobile scanner.

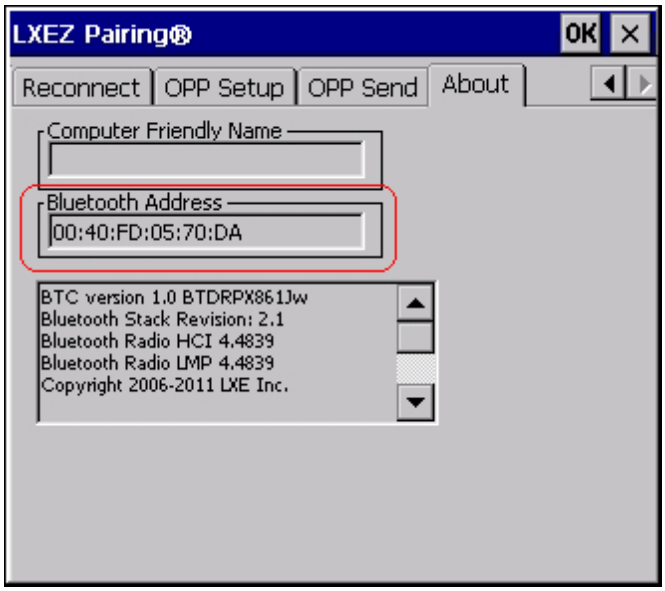
The devices are paired. The Bluetooth mobile barcode reader responds with a series of beeps and an LED flashes. Refer to the following section titled "Bluetooth Beep and LED Indications".

Note: After scanning the VX7 Bluetooth label, if there is no beep and no LED flash from the Bluetooth mobile device, the devices are currently paired.

VX7 without Label

If the VX7Bluetooth address barcode label does not exist, follow these steps to create a unique Bluetooth address barcode for the VX7:

First, locate the VX7 Bluetooth address by tapping **Start > Settings > Control Panel > Bluetooth > About** tab.



Next, create[1] a Bluetooth address barcode label for the VX7.

The format for the barcode label is as follows:

[1] Free barcode creation software is available for download on the World Wide Web. Search using the keywords "barcode create".

- Barcode type must be Code 128.
- FNC3 character followed by string Uppercase L, lowercase n, lowercase k, uppercase B and then the Bluetooth address (12 hex digits, no colons). See the sample barcode.

Create and print the label.

Scan the VX7 Bluetooth address barcode label with the Bluetooth barcode reader.

The devices are paired. The Bluetooth barcode reader responds with a series of beeps and LED flashes.

Note: After scanning the VX7 Bluetooth label, if there is no beep and no LED flash from the Bluetooth barcode reader, the devices are currently paired.

See Also: "Bluetooth Beep and LED Indications"

Bluetooth Beep and LED Indications

Beep Type from Bluetooth Device	Behavior
Acknowledge label	1 beep
Label rejected	2 beeps at low frequency
Transmission error	Beep will sound high-low-high-low
Link successful	Beep will sound low-medium-high
Link unsuccessful	Beep will sound high-low-high-low

LED on Bluetooth Device	Behavior
Yellow LED blinks at 2 Hz	Linking in progress
Off	Disconnected or unlinked
Yellow LED blinks at 50 Hz	Bluetooth transmission in progress
Yellow LED blinks at the same rate as the paging beep (1 Hz)	Paging
Green LED blinks once a second	Disabled indication

Upon startup, if the scanner sounds a long tone, this means the scanner has not passed its automatic Selftest and has entered isolation mode. If the scanner is reset, the sequence is repeated. Contact Technical Assistance for information.

Bluetooth Printer Setup

The Bluetooth managed device should be as close as possible, in direct line of sight, with the VX7 during the pairing process.

1. Open the LXEZ Pairing Panel.
2. Tap **Discover**. Locate the Bluetooth printer in the Discovery panel.
3. Tap and hold the stylus (or doubletap) on the Bluetooth printer ID until the right-mouse-click menu appears.
4. Select **Pair as Printer** to pair the VX7 with the Bluetooth managed printer.

The devices are paired. The Bluetooth managed printer may respond with a series of beeps or LED flashes.

Please refer to the Bluetooth managed printer manufacturer's User Guide; it may be available on the manufacturer's web site. Contact Technical Assistance for Bluetooth product assistance.

Note: If there is no beep or no LED flash from the Bluetooth managed printer, the VX7 and the printer are currently paired.

Easy Pairing and Auto-Reconnect

The Bluetooth module can establish relationships with new devices after the user taps the Discover button. It can auto-reconnect to devices previously known but which have gone out of range and then returned within range. See Also: "Reconnect"

Note: Configuration elements are persistent and stored in the registry.

Setup the Bluetooth module to establish how the user is notified by easy pairing and auto-reconnect events.

AppLock, if installed, does not stop the end-user from using the Bluetooth application, nor does it stop other Bluetooth-enabled devices from pairing with the VX7 while AppLock is in control.

Using OPP

Pairing with an OPP Device

Prerequisites

- A remote device, such as a mobile phone, that supports OPP.
- OPP is enabled on the VX7.

How To

1. Place the remote device in discovery or visible mode.
2. Initiate discovery on the VX7 by tapping the **Discover** button on the **OPP Send** tab.
3. The VX7 discovers the remote device.
4. The VX7 attempts to send a file to the remote device.
5. The remote device prompts the user for a 4 digit PIN.
6. User enters the PIN.
7. The VX7 prompts the user for a 4 digit PIN.
8. User must enter the *same* PIN code as entered on the remote device.
9. The VX7 now pairs with the remote device.

Remote Device Pushes File to VX7

This section assumes that a device supporting OPP is paired with the VX7.

If a duplicate filename is received, LXEZ Pairing writes the file in the specified location, with an incremental number appended to the file name. For example, if a file named **file.jpg** is pushed to the VX7 and that filename already exists in the Inbox, LXEZ Pairing saves the new file as **file001.jpg**. If the same file is pushed again, it is saved as **file002.jpg**.

There are several scenarios based on configuration options on the **OPP Setup** tab.

Notifications enabled, VX7 is Write Capable

1. The OPP client initiates a connection to the VX7 by selecting a file to push to the VX7.
2. The VX7 user is notified that a File Push request has been issued from a remote device.
3. The VX7 user is prompted to accept or reject the incoming request.
4. If the user accepts the request:
    a. The file is pushed to the VX7.
    b. LXEZ Pairing notifies the user that a file has been received.
    c. The connection is closed by the remote device (OPP client).
5. If the user rejects the request:
    a. The file is not pushed to the VX7.
    b. The connection is closed.

Notifications enabled, VX7 is not Write Capable

1. The OPP client initiates a connection to the VX7 by selecting a file to push to the VX7.
2. The file is rejected silently (no notification to the VX7 user).

Notifications disabled, VX7 is Write Capable

1. The OPP client initiates a connection to the VX7 by selecting a file to push to the VX7.
2. The file is accepted silently (no notification to the VX7 user).

Notifications disabled, VX7 is not Write Capable

1. The OPP client initiates a connection to the VX7 by selecting a file to push to the VX7.
2. The file is rejected silently (no notification to the VX7 user).

VX7 Pushes File to Remote Device

This section assumes that a device supporting OPP is paired with the VX7.

The VX7 (OPP client) initiates a connection to the remote device (OPP server) by selecting a file to push to the remote device. The VX7 sends the file and disconnects. The remote device may prompt the user (of that remote device) to accept the incoming request depending on the security settings of the remote device. The prompt may be displayed more than once, or it may not be displayed at all.

Notifications enabled

The file is pushed to the remote device and the user of the VX7 is notified of the completion of the push.

Notifications disabled

The file is pushed to the remote device and the user of the VX7 is not notified of the completion of the push.

LXEZ Pairing and External Application

Because only one application can use the OPP service at a time, external applications that wish to use OPP should disable LXEZ Pairing OPP before using the OPP service and restore LXEZ Pairing OPP upon completion using available API calls (see the *CE API Programming Guide* for details). These API calls are the equivalent of checking or unchecking the Disable LXEZ Pairing OPP checkbox.

- If Disable LXEZ Pairing OPP is not checked, checking it causes LXEZ Pairing OPP to be disabled and the send and receive functionality is disabled.
- If Disable LXEZ Pairing OPP is checked, and no application has registered a callback, un-checking LXEZ Pairing OPP enables OPP functionality in LXEZ Pairing, and the send and receive functionality is enabled.
- If Disable LXEZ Pairing OPP is checked, and another application has registered a callback, un-checking Disable LXEZ Pairing OPP issues a dialog box which says "Another application is using OPP. Do you wish to force their disconnection? Doing so will force the other application to be unregistered." The application that has been forcibly unregistered receives a FORCED_UNREGISTER_RECEIVED event.

Certificates

Start > Settings > Control Panel > Certificates

Manage digital certificates used for secure communication.

Note: Digital certificates are date sensitive. If the date on the VX7 is incorrect, wireless authentication will fail.

The Certificates stores lists the certificates trusted by the VX7 mobile device user.

These values may change based on the type of network security resident in the client, access point or the host system.

Tap the **Import** button to import a digital certificate file.

Tap the **View** button to view a highlighted digital certificate.

Tap the **Remove** button to remove highlighted certificate files.

Tap the ? button and follow the instructions in the Windows CE Help file when working with trusted authorities and digital certificates.

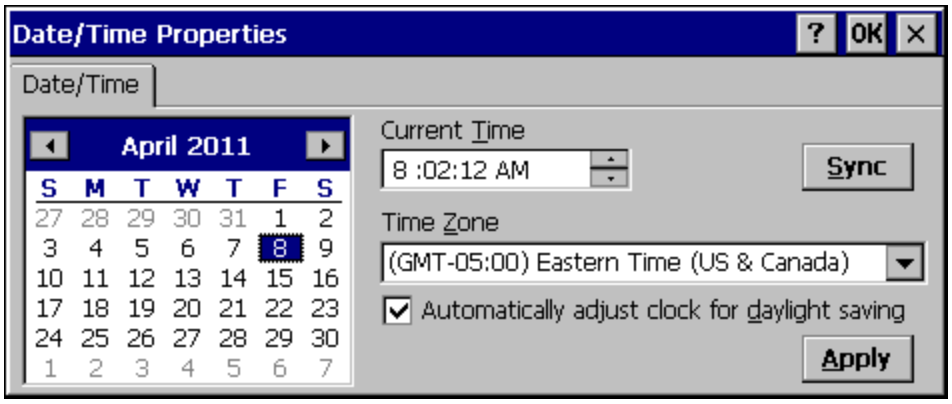
Date / Time

Start > Settings > Control Panel > Date/Time - or - Time in Desktop Taskbar

Use this VX7 panel to set Date, Time, Time Zone, and assign a Daylight Savings location.

Factory Default Settings

Current Time	Midnight
Time Zone	GMT-05:00
Daylight Savings	Enabled


Date/Time Properties
?
OK
Date/Time
April 2011
S M T W T F S
27 28 29 30 31 1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
1 2 3 4 5 6 7
Current Time
8 :02:12 AM
Sync
Time Zone
(GMT-05:00) Eastern Time (US & Canada)
Automatically adjust clock for daylight saving
Apply

There is very little functional change from general desktop or laptop Date/Time Properties options.

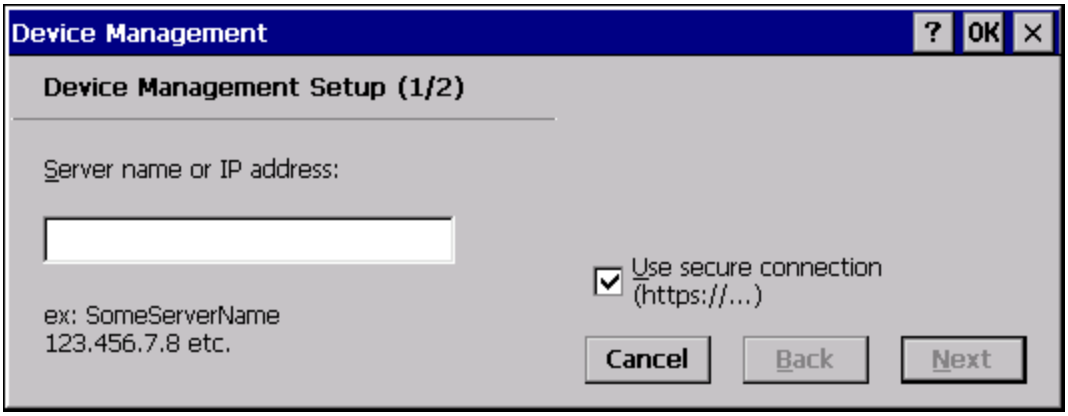
Double-tapping the time displayed in the Desktop Taskbar causes the Date/Time Properties screen to appear.

The Sync button activates a utility that will set the clock using a network time server.

Device Management

Start > Settings > Control Panel > Device Management

Allows a Device Management client (the device equipped with a Microsoft Windows CE operating system) to work with a Microsoft Systems Management Server.



Specify the server name or IP address of management server and check the checkbox if a secure connection is to be used.

Refer to the Microsoft.com website for more information on device management for Windows CE equipped devices.

Dialing

Start > Settings > Control Panel > Dialing

Set dialup properties for internal modems (not supplied or supported on the VX7).

Factory Default Settings

Location	Work
Area Code	425
Tone Dialing	Enabled
Country/Region	1
Disable Call Waiting	Disabled (blank)

Display

Start > Settings > Control Panel > Display

The display might also called the touch screen.

Select the desktop background image and appearance scheme for the VX7. Using the options on the Backlight tab, set the display backlight and keypad backlight timers when running on battery or external power.

Adjust the settings and tap the OK button to save the changes. Saved changes take effect immediately.

Factory Default Settings

Background	
Image	Windows CE
Image on background	Disabled
Appearance	
Schemes	Windows Standard
Backlight	
Battery power	Never
External power and user idle	Never

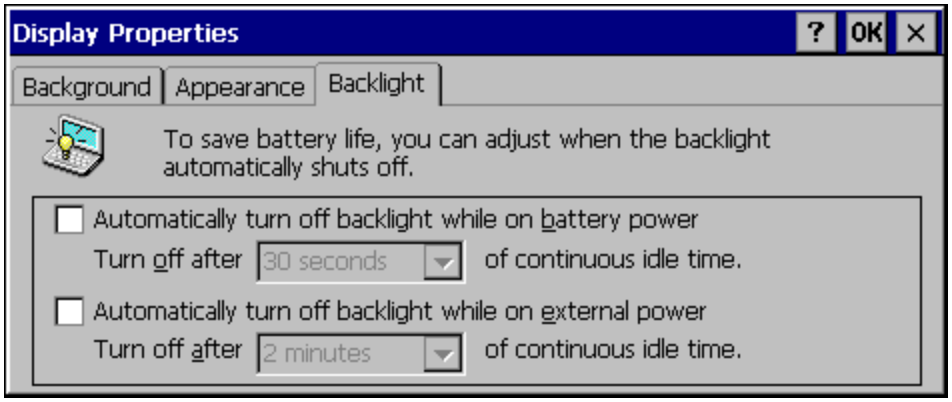
Background

There is very little change from general desktop PC Display Properties / Background options. Select an image from the dropdown list (or tap the Browse button to select an image from another folder) to display on the Desktop, and then tap the OK button to save the change. The change takes effect immediately.

Appearance

There is very little change from general desktop PC Appearance options. Select a scheme from the dropdown list and make changes to the parameters. The default is High Contrast White for monochrome displays and Windows Standard for color displays. Tap the Save button to save any changes, renaming the scheme if desired. Tap the Delete button to delete schemes. Tap the Apply button to apply the selected scheme to the display.

Backlight



The backlight settings use the default timeouts and are synchronized to the User Idle setting in the Schemes tab in the Power control panel.

When the backlight timer expires, the touch screen backlight is dimmed, not turned off. When both checkboxes are unchecked, the backlight never turns off (or dims).

Default values are disabled for battery and external power. By default the backlight is always on.

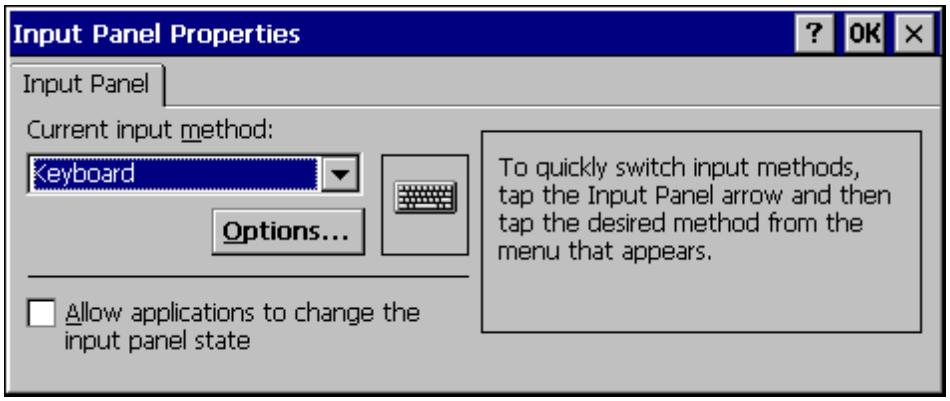
Input Panel

Start > Settings > Control Panel > Input Panel

Set the current VX7 keys and data input method.

Factory Default Settings

Input Method	Keyboard
Allow applications to change input panel state	Enabled
Options button	
Keys	Small keys
Use gestures	Disabled


Input Panel Properties
?
OK
Input Panel
Current input method:
Keyboard
Options...
To quickly switch input methods, tap the Input Panel arrow and then tap the desired method from the menu that appears.
Allow applications to change the input panel state

Use this panel to make the Input Panel (on-screen keyboard) or the physical keypad primarily available when entering data on any screen.

Selecting Keyboard enables both.

Tap the Options button to set the size of the keys displayed on-screen and whether Transcriber gestures are enabled or disabled.

Note: Contact Technical Assistance for language pack availability.

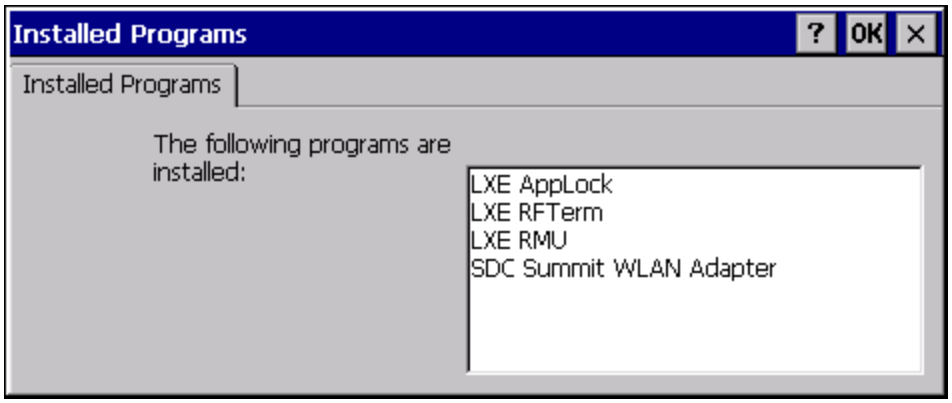
Installed Programs

Start > Settings > Control Panel > Installed Programs

Note: Lists programs installed in RAM.

View the list of installed programs. No user interaction is required.

In some OS versions, this panel replaces Remove Programs.



Note: Contact Technical Assistance if installed programs must be deleted.

Internet Options

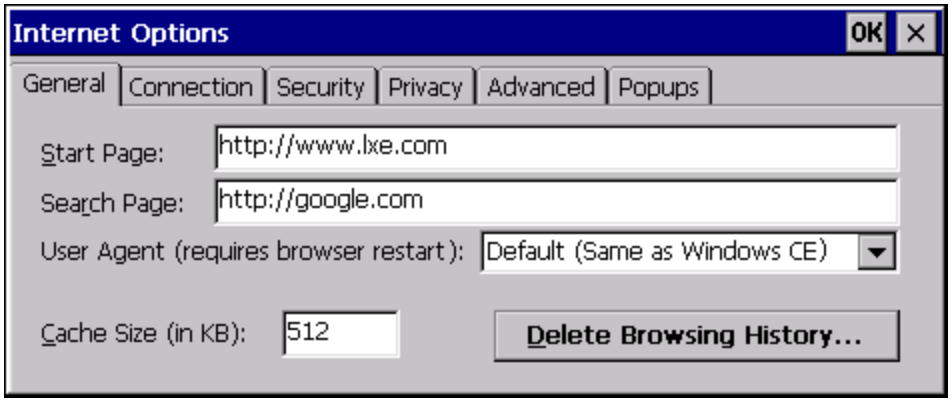
Start > Settings > Control Panel > Internet Options

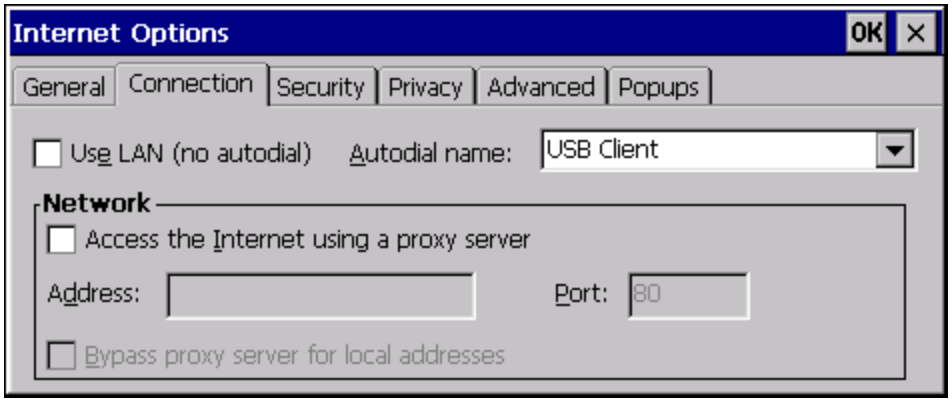
Set options for VX7 Internet connectivity.

Select a tab. Tap the ? button for help using Windows CE Help installed in your mobile device. Adjust the settings and tap the OK button. The changes take effect immediately.

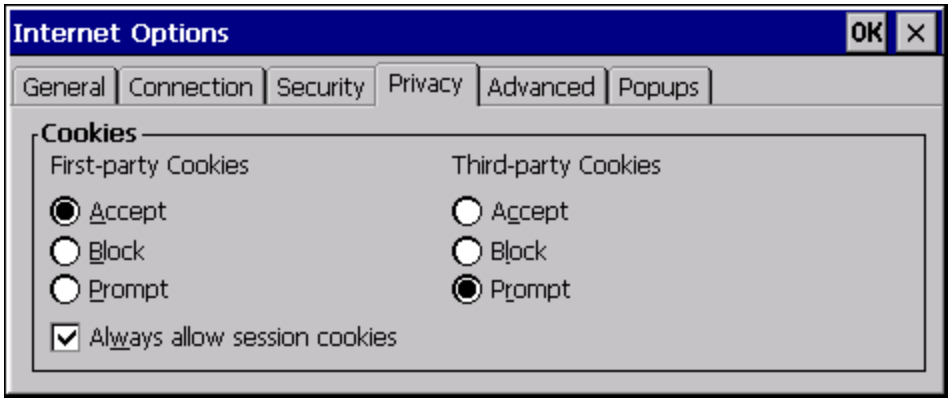
Factory Default Settings

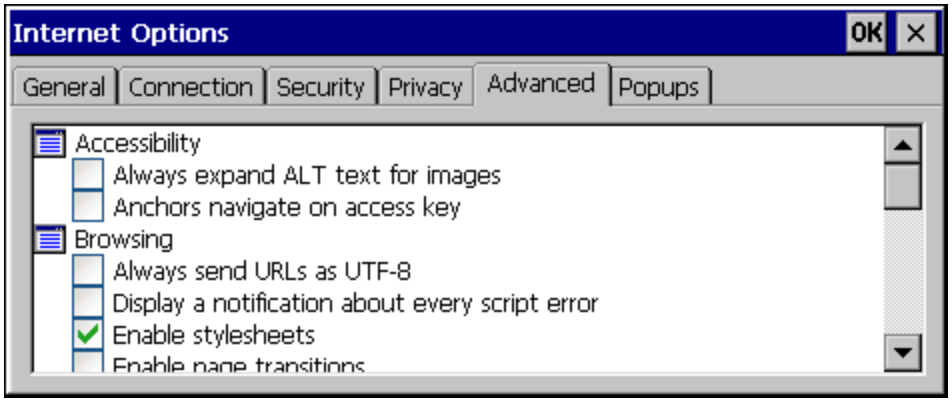
General	
Start Page	http://www.lxe.com/
Search Page	http://www.google.com
Cache Size	512Kb
Connection	
Use LAN	Disabled
Autodial Name	Blank
Proxy Server	Disabled
Bypass Proxy	Disabled
Security	
Allow cookies	Enabled
Allow TLS 1.0 security	Disabled
Allow SSL 2.0 security	Enabled
Allow SSL 3.0 security	Enabled
Warn when switching	Enabled
Privacy	
First party cookies	Accept
Third party cookies	Prompt
Session cookies	Always allow
Advanced	
Stylesheets	Enabled
Theming Support	Enable
Multimedia	All options enabled
Security	All options enabled
Popups	
Block popups	Disabled
Display notification	Enabled
Use same window	Disabled

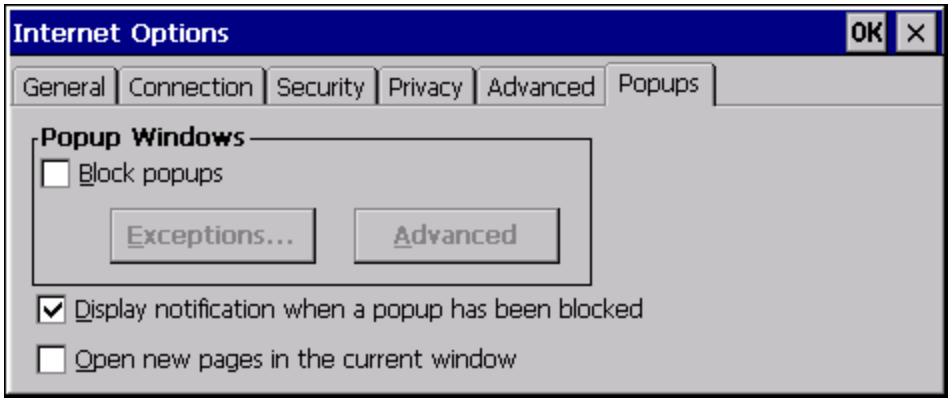

Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Start Page:
http://www.lxe.com
Search Page:
http://google.com
User Agent (requires browser restart):
Default (Same as Windows CE)
Cache Size (in KB):
512
Delete Browsing History...


Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Use LAN (no autodial)
Autodial name:
USB Client
Network
Access the Internet using a proxy server
Address:
Port:
80
Bypass proxy server for local addresses

Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Internet
Local intranet
Trusted sites
Restricted sites
Sites...
Settings...
Internet
This zone contains all Web sites you haven't placed in other zones


Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Cookies
First-party Cookies
Accept
Block
Prompt
Always allow session cookies
Third-party Cookies
Accept
Block
Prompt


Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Accessibility
Always expand ALT text for images
Anchors navigate on access key
Browsing
Always send URLs as UTF-8
Display a notification about every script error
Enable stylesheets


Internet Options
OK
General
Connection
Security
Privacy
Advanced
Popups
Popup Windows
Block popups
Exceptions...
Advanced
Display notification when a popup has been blocked
Open new pages in the current window

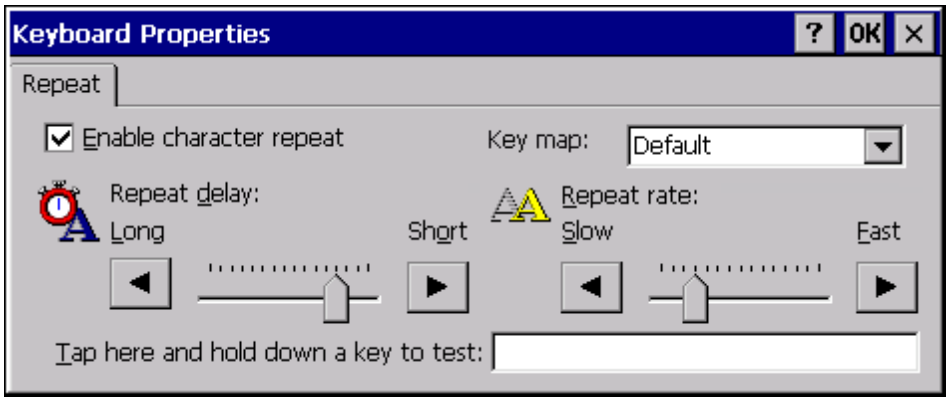
Keyboard

Start > Settings > Control Panel > Keyboard

Set keypad key map, keypad key repeat delay, and key repeat rate.

Factory Default Settings

Repeat Tab	
Key map	Default (or Default VX7)
Repeat character	Enable
Repeat Delay	Short
Repeat Rate	Slow



Select a key map using the drop-down list. Adjust the character repeat settings and tap the OK button to save the changes.

When new key maps, or fonts, are added to the registry, they are available immediately and the font name is in the Keyboard Properties Key map dropdown list. Only one font at a time can be selected. The fonts affect the screen display, they do not affect any virtual (touch screen) key taps.

See **About > Software > Language** tab for the name of any installed fonts.

KeyPad

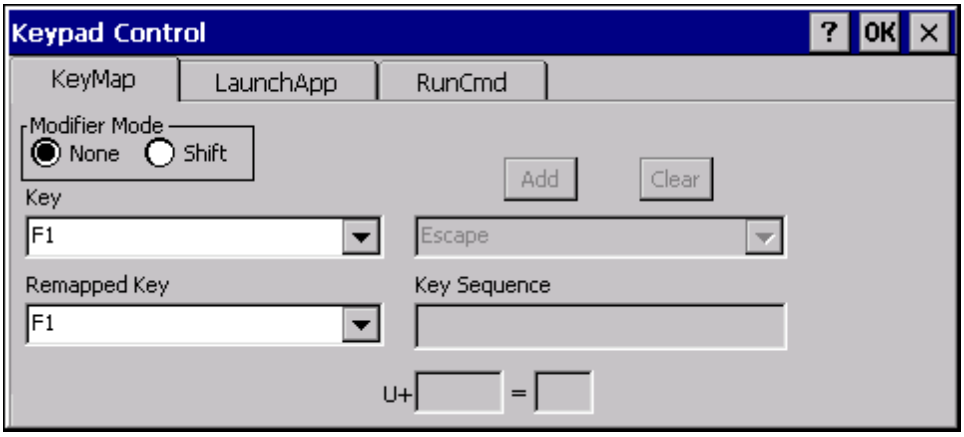
Start > Settings > Control Panel > KeyPad Icon

Use this control panel option to assign key functions to mappable keys available on your VX7, determine application launch sequences and program command Run sequences.

Note: KeyPad Control Panel options LaunchApp and RunCmd do not inter-relate with similarly-named options contained in other Control Panel applets. For example, the AppLock Administrator Control panel file Launch option.

Factory Default Settings		
KeyMap		
Modifier Mode	None	
Key	F1	Remap to – F1
Edit String	Field Exit	String – Empty
LaunchApp		
App1	Empty	
App2	Empty	
App3	Empty	
App4	Empty	
App/Opt	EXE	
RunCmd		
Cmd1	Empty	
Cmd2	Empty	
Cmd3	Empty	
Cmd4	Empty	
File/Parm	FILE	

KeyMap Tab



Assign settings by clicking radio buttons and selecting keys from the drop down boxes. Tap the OK button when finished. The changes take effect immediately.

Remap a Single Key

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select the value from the remapped key from the Remapped Key pulldown list.
4. Click **OK** to save the result and close the control panel.

Remap a Key to a Unicode Value

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select **Unicode** from the Remapped Key pulldown list.
4. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
5. Click **OK** to save the result and close the control panel.

Remap a Key Sequence

Up to 16 keys may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select **Key Sequence** from the Remapped Key pulldown list.
4. Select the first key for the multiple key sequence from the pulldown list.
5. Press the **Add** button to add the key to the multiple key sequence shown in the Key Sequence box.

6. Repeat this steps 4 and 5 until all desired keys have been added to the key sequence. If necessary, use the **Clear** button to erase all entries in the Key Sequence box.
7. Click **OK** to save the result and close the control panel.

Note: A key can only be used once in a multiple key sequence. For example, an F1 key added to a key sequence means an F1 key cannot be used again in the same key sequence.

Remap a Key to a Sequence of Unicode Values

Up to 16 Unicode values may be specified for the key sequence. The sequence can consist of keys and Unicode values.

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select **Key Sequence** from the Remapped Key pulldown list.
4. Select **Unicode** from the Key Sequence pulldown list.
5. There are two Unicode text boxes located on the lower part of this tab. Enter the Unicode value in the left textbox and the Unicode character is displayed in the right textbox.
6. Press the **Add** button to add the key to the multiple key sequence shown in the Key Sequence box.
7. Repeat this steps 4 through 6 until all desired characters have been added to the key sequence. If necessary, use the **Clear** button to erase all entries in the Key Sequence box.
8. Click **OK** to save the result and close the control panel.

Remap an Application

1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select Launch App1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on the LaunchApp tab.
5. Make sure the EXE radio button is selected.
6. In the text box (App1-4) corresponding to the number selected for Launch App1-4, enter the application to launch.
7. If any parameters are needed for the application, click on the OPT radio button. This clears the text box (though the application name is saved). Enter the desired parameters in the appropriate text box.
8. Click OK to save the result and close the control panel.
9. If the KeyMap tab is accessed again, the application plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

Remap a Command

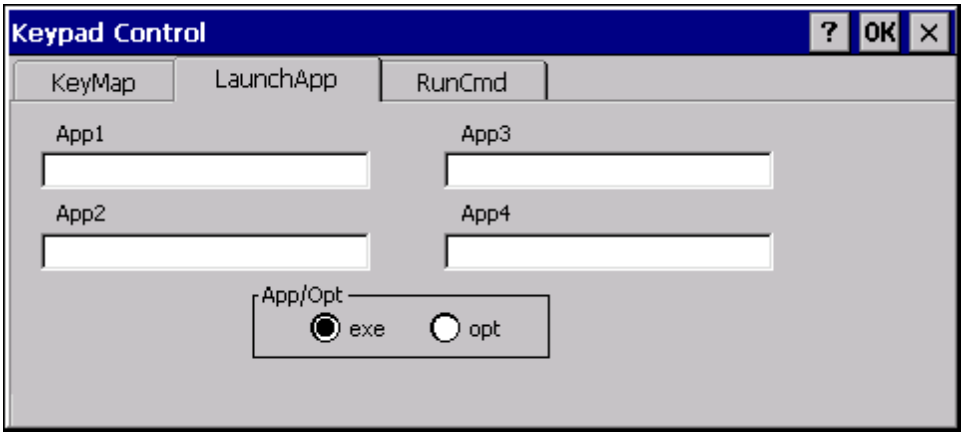
1. Select the modifier key from the Modifier Mode options.
2. Select the key to be remapped from the Key pulldown list.
3. Select RunCmd 1-4 from the remapped key from the Remapped Key pulldown list.
4. Click on the RunCmd tab.
5. Make sure the FILE radio button is selected.
6. In the text box (Cmd1-4) corresponding to the number selected for RunCmd1-4, enter the desired command.
7. If any parameters are needed for the command, click on the PARM radio button. This clears the text box (though the command is saved). Enter the desired parameters in the appropriate text box.

8. Click OK to save the result and close the control panel.
9. If the KeyMap tab is accessed again, the command plus any specified parameters is displayed in the Key Sequence text box when the remapped key is again selected.

LaunchApp Tab

The default for all text boxes is Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the VX7 emits a single beep, if the launch is successful, it is silent.



The Launch App command is defined for use by system administrators. These instructions are parsed and executed directly by the keyboard driver.

1. Place the cursor in the text box next to the App you wish to run, e.g. App1, App2.
2. Enable the EXE radio button if the application is an EXE file.
3. Enter the name of the executable file.
4. Enable the OPT radio button to add options or parameters for the executable file in the same text box. Switching from EXE to OPT clears the text box (but the information previously entered is stored), allowing parameter entry.

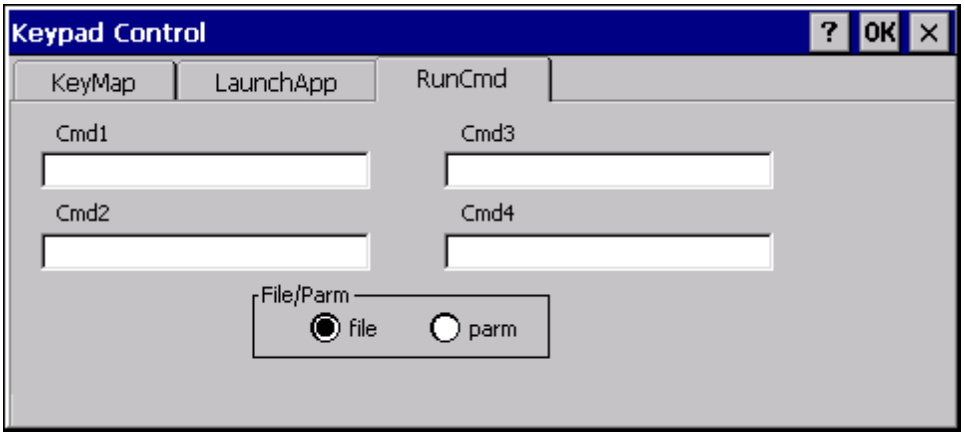
Tap the OK button when finished. The changes take effect immediately.

The result of the application (exe) and options (opt) entries are displayed on the KeyMap tab in the Key Sequence box when the key mapped to the LauchApp is selected.

RunCmd Tab

The default for all text boxes is Empty, Null or " ". The text boxes accept string values only.

Note that executables and parameters are not checked for accuracy by the keyboard driver. If the launch fails, the VX7 emits a single beep, if the launch is successful, the mobile device is silent.



The Run Cmd command is defined for use by system administrators. These instructions call the ShellExecuteEx API, which opens documents directly.

1. Place the cursor in the text box next to the Cmd you wish to run, e.g. Cmd1, Cmd2.
2. Enable the file radio button and enter the name of the file.
3. Enable the PARM radio button to add parameters for file/exe execution in the same text box.

Tap the OK button when finished. The changes take effect immediately.

License Viewer

Start > Settings > Control Panel > License Viewer

Use this option to view software license registration details, and service contract length for VX7. Information on the License Viewer tabs is unique for each VX7.

Note: Following image is a sample screen.

Your License Viewer control panel may show more tabs, e.g. RFTerm, depending on the number of software applications running on the VX7 that require a license. Contact Technical Assistance for software updates and releases as they become available.

Software and driver version information is located in the About control panel. Copyright information is located in the System control panel.

Mixer

Start > Settings > Control Panel > Mixer

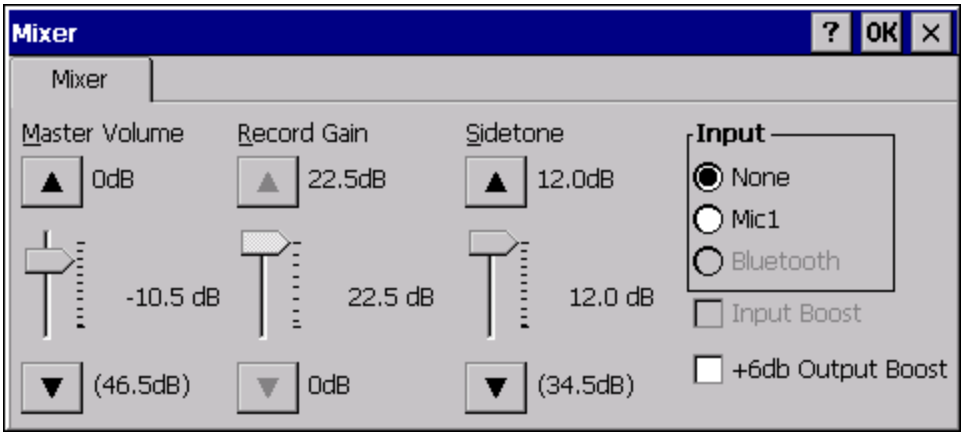
The VX7 has a pair of speakers. They are active when a headset is not connected to the device.

Use the settings on these panels to adjust the volume, record gain and sidetone for microphone input, speaker and speaker output.

Headsets can be enabled, disabled and selected using these panels.

Factory Default Settings

Master Volume	-10.5 dB
Record Gain	22.5 dB
Sidetone	12.0 dB
Input	None
Input Boost	Dimmed
+6db Output Boost	Disabled



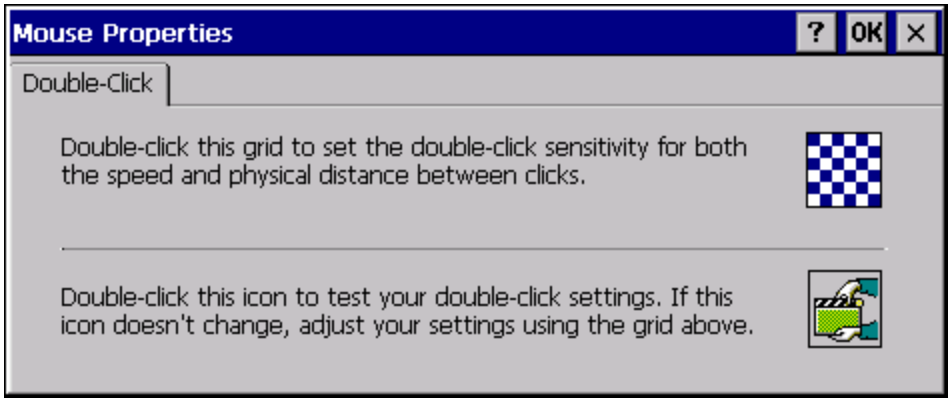
Select the input for the mixer. Move the sliders up and down, or tap the up and down arrows, to adjust the decibel level.

*Note: Set Input to **None** when using stereo headphones. Set Input to **Mic1** when using a mono headset with microphone.*

Mouse

Start > Settings > Control Panel > Mouse

Use this option to set the double-tap sensitivity for stylus taps on the VX7 touch screen.


Mouse Properties
?
OK
Double-Click
Double-click this grid to set the double-click sensitivity for both the speed and physical distance between clicks.
Double-click this icon to test your double-click settings. If this icon doesn't change, adjust your settings using the grid above.

MX3X-VXC Options

Start > Settings > Control Panel > MX3X-VXC Options

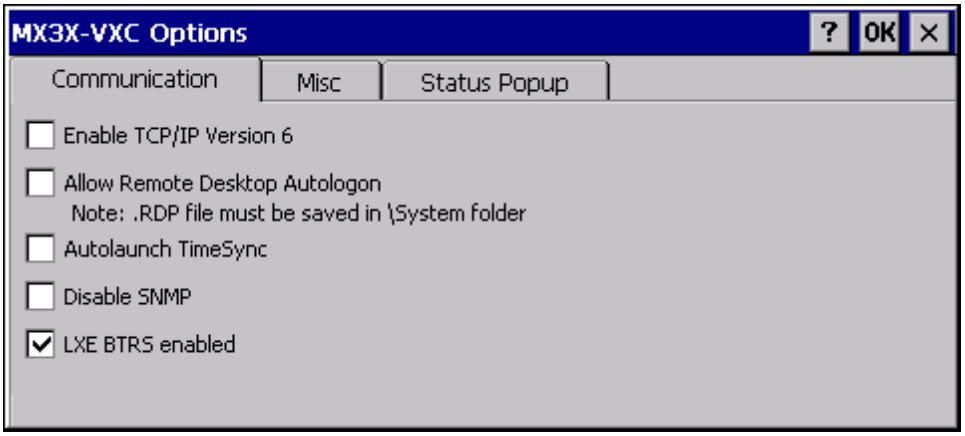
Set options such as IP V6, time sync, touch screen enable and CapsLock. Also set Status Popup taskbar icon display options for the Admin and User.

It may be necessary to warmboot the VX7 after making desired changes. A pop up window indicates if a warmboot is required.

Note: Contact Technical Assistance for upgrade details If there is no icon corresponding to this item in the Control Panel.

Communication

Options on this tab configure communication options for the VX7.



Enable TCP/IP Version 6

By default, IPv6 is disabled on the VX7. Click this checkbox to enable IPv6.

Allow Remote Desktop Autologon

By default, Remote Desktop Autologon is disabled. Click this checkbox to enable Remote Desktop Autologon.

Note: The .RDP file must be saved in the \System folder. When prompted, use the Save As button to save the .RDP file is the \System folder. If the .RDP file is saved in the default root folder location, the .RDP file will not persist across a warmboot.

Autolaunch TimeSync

By default, TimeSync does not automatically run on the VX7. To enable TimeSync to run automatically on the VX7, click this checkbox.

Synchronize with a Local Time Server

By default, GrabTime synchronizes via an Internet connection. To synchronize with a local time server:

1. Use ActiveSync to copy GrabTime.ini from the **My Device > Windows** folder on the mobile device to the host PC.
2. Edit the copy of GrabTime.ini on the host PC. Add the local time server's domain name to the beginning of the list of servers. You can optionally delete the remainder of the list.
3. Copy the modified GrabTime.ini file to the **My Device > System** folder on the mobile device.

The System/GrabTime.ini file takes precedence over the Windows/GrabTime.ini file. System/Grabtime.ini also persists after a coldboot; Windows/Grabtime.ini does not persist.

Disable SNMP

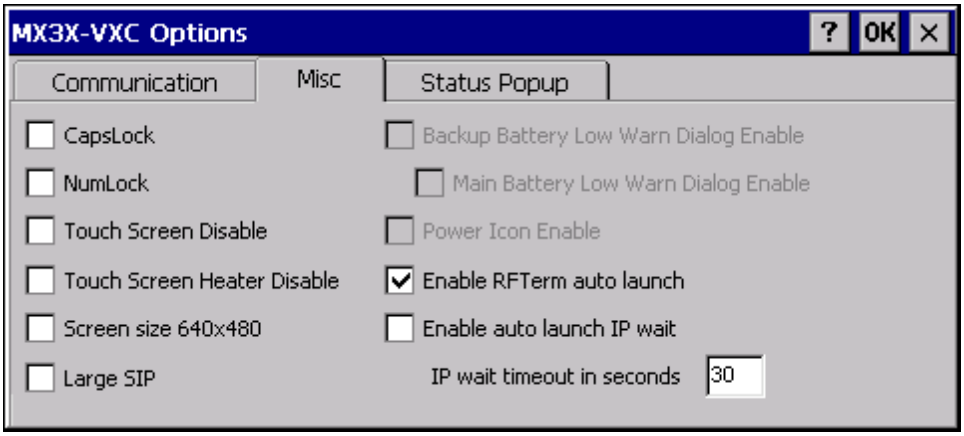
By default, the SNMP agent is running on the VX7. To disable the SNMP agent, check this box.

LXE BTRS Enabled

By default, the VX7 uses proprietary handshaking designed for the Honeywell Bluetooth Ring Scanner. Uncheck this box to use the VX7 with a third party Bluetooth scanner.

Misc

Options on this tab configure device specific options. Note that options not available on the VX7 are dimmed or grayed out.



CapsLock

By default, CapsLock is disabled after a warmboot. To enable CapsLock after a warmboot, click this checkbox.

NumLock

By default, NumLock is disabled after a warmboot. To enable NumLock after a warmboot, click this checkbox.

Touch Screen Disable

By default, the VX7 touch screen is enabled. To disable the touch screen after a warmboot, click this checkbox.

Touch Screen Heater Disable

The touch screen heater is optional on the VX7.

By default, the touch screen heater is enabled. To disable the touch screen heater, click this checkbox. If the VX7 does not have a touch screen heater, this checkbox is dimmed.

Screen Size 640x480

By default, the display resolution is 800 x 600 pixels. Clicking this box enables the 640 x 480 pixel resolution. Clicking this box again toggles the display to 800 x 600 pixels.

Large SIP

The Software Input Panel (SIP, also called virtual keyboard) can be displayed in a standard size or a large size. By default, the smaller SIP is displayed. To enable the larger SIP, check this checkbox.

Enable RFTerm Auto Launch

This option is enabled by default. This option, when disabled (unchecked) stops RFTerm from launching at bootup. When RFTerm is not installed or has not been added to the registry *Launch* sequence, this checkbox is ignored at bootup.

Enable Auto Launch IP Wait

When enabled, this feature works as follows:

1. After the radio .CAB file is unpacked, the Launch program waits for the radio driver to load and for the radio to connect and obtain an IP address.
2. During the wait, a message window is displayed containing the NDIS communication messages up to and including the display of the valid IP address.
3. After the IP address is obtained, the message window is displayed for one second and then removed.
4. Launch completes its normal task path, unpacking any remaining .CAB files and completing any remaining tasks.
5. If an IP address is not obtained within the specified timeout period (see below), Launch completes its normal task path.

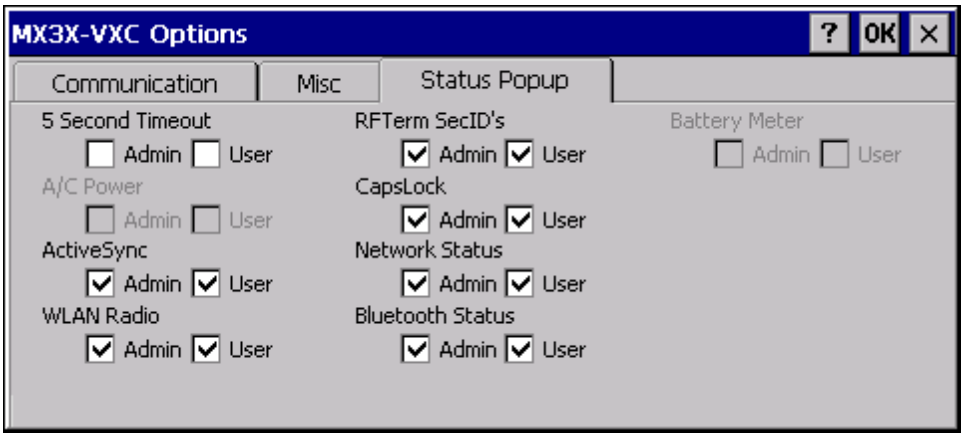
The default is unchecked (disabled). Launch does not wait for an IP address.

IP Wait Timeout

This parameter specifies the maximum time period Launch waits for a valid IP address before completing any remaining tasks. The timeout can be from 1 to 60 seconds. The default is 30 seconds.

Status Popup

Options on this tab configure the Status Popup window. When the Status popup window is displayed, it is placed on top of the window in focus and hides any data beneath it. It is closed by pressing the assigned Status User or Status Admin key sequence.



Using the key mapping control panel, the System Administrator must first assign a **Status User** key sequence for the end-user when they want to toggle the Status Popup Window on or off.

The System Administrator must also assign a **Status Admin** key sequence to perform the same function. Status popup window display options (taskbar icons) are assigned on the Status Popup tab, e.g., AC Power, ActiveSync, WLAN radio, CapsLock, Network status, Bluetooth status.

The default for the User and Admin status popup windows is to show all status information. The 5 second timeout to remove the status popup from the display is disabled by default for the User and Admin status popup windows.

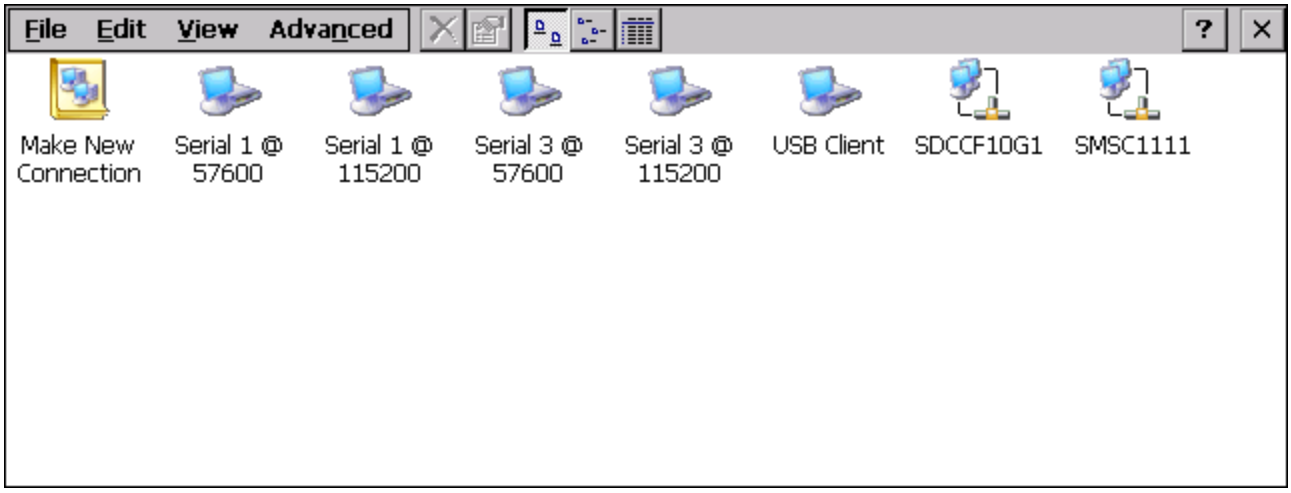
In addition to the configurable options, the Status Popup displays memory status information at the bottom of the popup window. The following information is displayed:

ml	Memory Load	Number indicating the estimate of current memory use, between 0 (no memory use) and 100 (full memory use)
tp	Total Physical memory	Bytes of total physical memory
ap	Available Physical memory	Bytes of available physical memory
tv	Total Virtual memory	Total bytes that can be described in the user mode portion of the virtual address space of the calling process.
av	Available Physical memory	Bytes of unreserved and uncommitted memory in the user mode portion of the virtual address space of the calling application.

Network and Dialup Options

Start > Settings > Control Panel > Network and Dialup Connections

Set VX7 network driver properties and network access properties. Select a connection to use, or create a new connection.



Create a New Connection

1. On the mobile device, select **Start > Settings > Control Panel > Network and Dialup Connections**. A window is displayed showing the existing connections.
2. Assuming the connection you want does not exist, double-tap **Make New Connection**.
3. Give the new connection an appropriate name (My Connection @ 9600, etc.). Tap the **Direct Connection** radio button. Tap the **Next** button.
4. From the popup menu, choose the port you want to connect to. Only the available ports are shown.
5. Tap the **Configure...** button.
6. Under the Port Settings tab, choose the appropriate baud rate. Data bits, parity, and stop bits remain at 8, none, and 1, respectively.
7. Under the **Call Options** tab, be sure to turn off Wait for dial tone, since a direct connection will not have a dial tone. Set the timeout parameter (default is 5 seconds). Tap **OK**.
8. **TCP/IP Settings** should not need to change from defaults. Tap the **Finish** button to create the new connection.
9. Close the **Remote Networking** window.
10. To activate the new connection select **Start > Settings > Control Panel > PC Connection** and tap the **Change Connection…** button.
11. Select the new connection. Tap **OK** twice.
12. Close the Control Panel window.
13. Connect the desktop PC to the mobile device with the appropriate cable.
14. Click the desktop **Connect icon** to test the new connection.

You can activate the connection by double-tapping on the specific connection icon in the Remote Networking window, but this will only start an RAS (Remote Access Services) session, and does not start ActiveSync properly.

Network Capture

Start > Settings > Control Panel > Network Capture

Note: Verify the date and time before using the logging utilities to ensure meaningful data.

The Network Capture panels provide configuration options for logging utilities.

Two types of logging are configurable:

Netlog is a Windows CE utility that monitors network traffic. Netlog creates a .CAP file that can be read using Microsoft Windows Network Monitor or any compatible tool that supports .CAP files.

NDISLog monitors the NDIS interface between the Summit radio and the NDIS driver. This utility creates a .TXT log file.

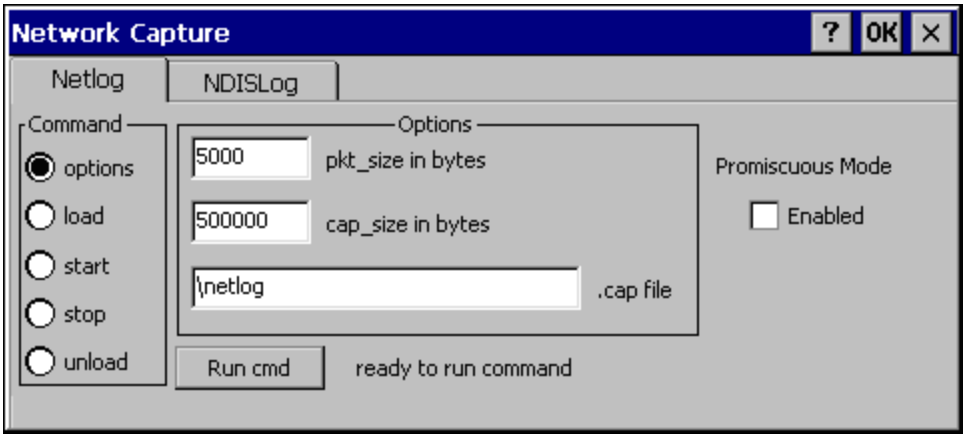
Factory Default Settings

Netlog	
Command	options
pkt_size in bytes	5000
cap_size in bytes	500000
.cap file	\netlog
Promiscuous Mode	Disabled
NDISLog	
Command	stop
file	\ndislog.txt

Netlog

Use this control panel to configure the Netlog utility. By configuring Netlog using the control panel, Netlog remains running across a warmboot. However, please note that:

- Netlog first stores data to a file named netlog0.cap, then netlog1.cap. Any time the current file reaches maximum size, Netlog switches to the other file.
- If the log file is stored in the root directory, any previous data is lost and a new log file started after the warmboot.
- If the log file is stored in \System, all previous data is saved across the warmboot.
- If Netlog is enabled across the warmboot, a series of brief popups may be displayed during the boot cycle. No user interaction is required.



Command

Command	Function
options	Specifies the option to perform. See the table below for the option parameters and values.
load	Loads and starts Netlog.
start	Starts the Netlog process of logging the network traffic.
stop	Stops Netlog from logging network traffic.
unload	Unloads Netlog.

Options

Options	Function
pkt_size in bytes	Specifies the maximum packet size captured in bytes. This option should only be run after you have called **load** and **stop**. Default is 5000.
cap_size in bytes	Specifies the maximum size of Netlog0.cap or Netlog1.cap in bytes. This option should only be run after you have called **load** and **stop**. Default is 500,000.
.cap file	Specifies the name of the file to which network traffic information is saved. This option should only be run after you have called **load** and **stop**. Default is \netlog.

Run cmd

Performs the command selected. For example, to run Netlog and modify the packet size do the following:

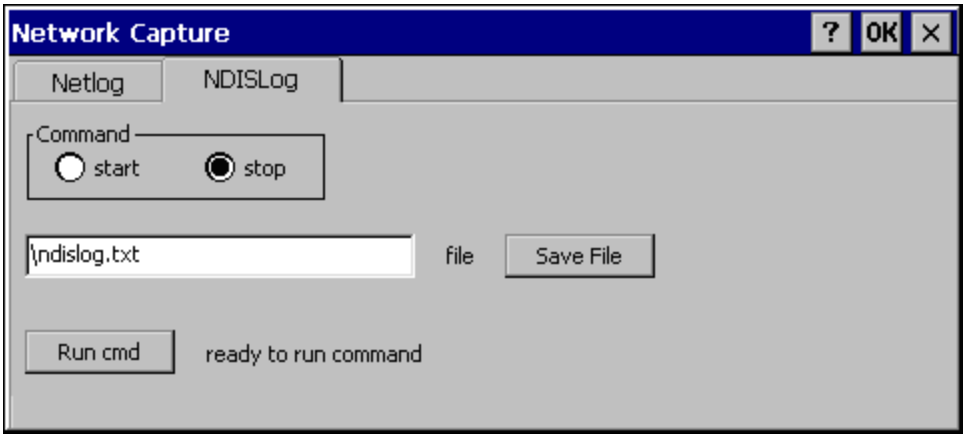
Select **load** from the Commands list and click the **Run cmd** button.

Select **stop** from the Commands list and click the **Run cmd** button.

Select **options** from the Commands list, enter the new packet size in the Options list and click the **Run cmd** button.

NDISLog

NDISLog creates a .TXT file that can be viewed with any text editor program that supports .TXT files.



Command

Command	Function
start	Starts logging the network traffic.
stop	Stops logging network traffic.

file

Specifies the name of the file to which NDISLog information is stored.

Save File

Stores the file name.

Run cmd

Performs the selected start or stop command.

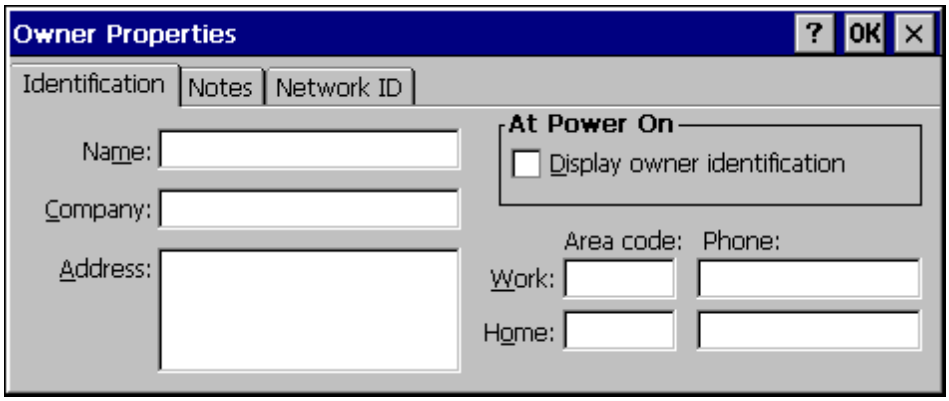
Owner

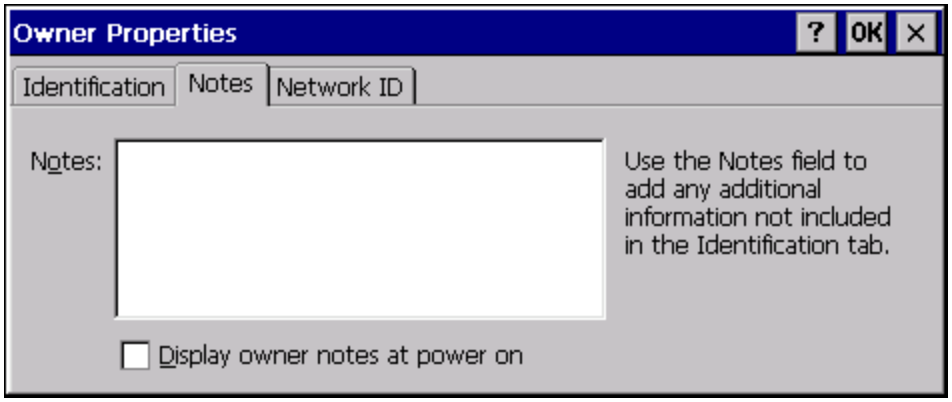
Start > Settings > Control Panel > Owner

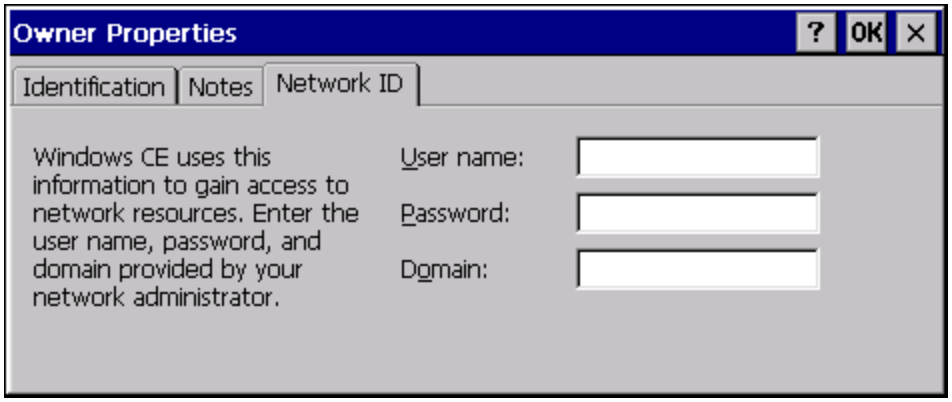
Set the VX7 owner details. The Network ID is used when logging into a remote network.

Factory Default Settings

Identification	
Name	Blank
Company	Blank
Address	Blank
Telephones	Blank
Display owner ID at power-on	Disabled
Notes	
Notes	Blank
Display notes at power-on	Disabled
Network ID	
User Name	Blank
Password	Blank
Domain	Blank







Enter user name, password and domain to be used when logging into network resources.

Password

Start > Settings > Control Panel > Password

Use this panel to set VX7 user access to control panels and power up password properties.

This password must be entered before performing a cold boot.

Contact Technical Assistance if entering a power-on or screen saver password does not allow you to disable this password protection or perform a cold boot.

Factory Default Settings

Password	Blank
Enter password at Power On	Disabled
Enter password at Remote Desktop Screen Saver	Disabled

- The password and password settings are saved during a warm boot and a cold boot.
- The screensaver password affects the Remote Desktop screensaver only.
- After a password is assigned and saved, each time a **Settings > Control Panel** option is selected, the user will be required to enter the password before the Control Panel will open.
- The screensaver password is the same as the power-on password. They are not set independently.
- A screensaver password cannot be created without first enabling the “Enable password protection at power-on” checkbox.
- The screensaver password is not automatically enabled when the “power-on” checkbox is enabled.

Enter the password in the Password text box, then press Tab and type the password again to confirm it.

Enable the power-on checkbox and, if desired, the screensaver checkbox.

A changed/saved password is in effect immediately.

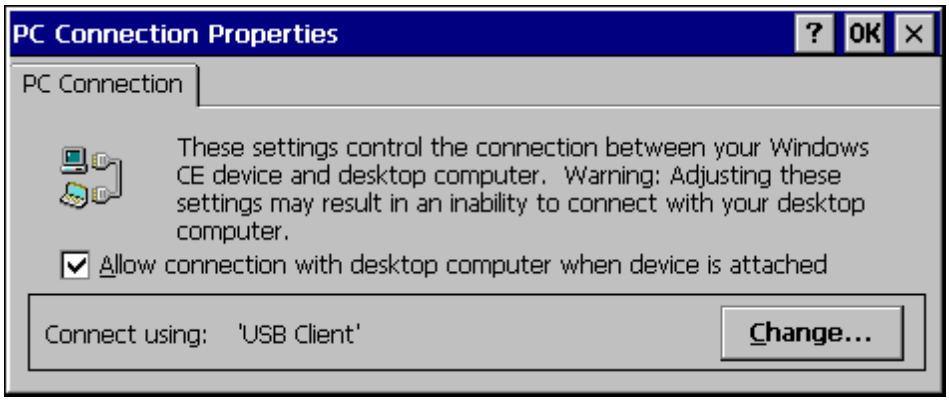
PC Connection

Start > Settings > Control Panel > PC Connection

Use these options to control a cabled connection (USB, serial) between the VX7 and a nearby desktop/laptop computer.

Factory Default Settings

Enable direct connection	Enabled
Connect using	USB Client


PC Connection Properties
?
OK
PC Connection
These settings control the connection between your Windows CE device and desktop computer. Warning: Adjusting these settings may result in an inability to connect with your desktop computer.
Allow connection with desktop computer when device is attached
Connect using: 'USB Client'
Change...

Unchecking the **Allow connection with desktop computer when device is attached** checkbox disables ActiveSync on the VX7.

Tap the **Change** button to change the direct connect setting.

Tap the drop-down box to view a list of pre-configured connection settings.

PCMCIA

Start > Settings > Control Panel > PCMCIA

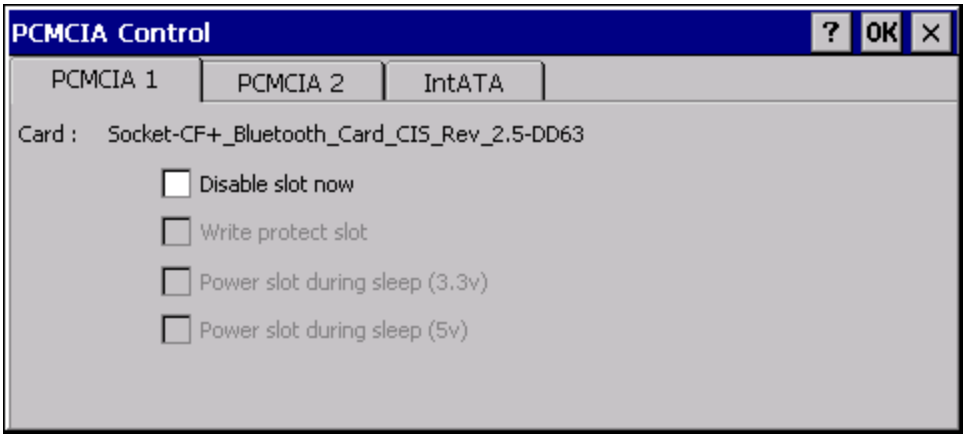
Use the options on the tabs to manage cards installed in the VX7.

Note: On the VX7 the PCMCIA 2 tab is for the card in the lower slot, labeled "PCMCIA B". PCMCIA 1 is the upper slot, labeled "PCMCIA A".

Factory Default Settings

PCMCIA 1	
Disable slot now	Off
Power slot during sleep (3.3v)	Dimmed
Power slot during sleep (5v)	Off
Write protect slot	Off (dimmed)
PCMCIA 2	
Disable slot now	Off
Power slot during sleep (3.3v)	(Off) Dimmed
Power slot during sleep (5v)	Off
Write protect slot	Off
IntATA	
Disable slot now	Off (dimmed)
Power slot during sleep (3.3v)	On (dimmed)
Power slot during sleep (5v)	Off (dimmed)
Write protect slot	Off (dimmed)

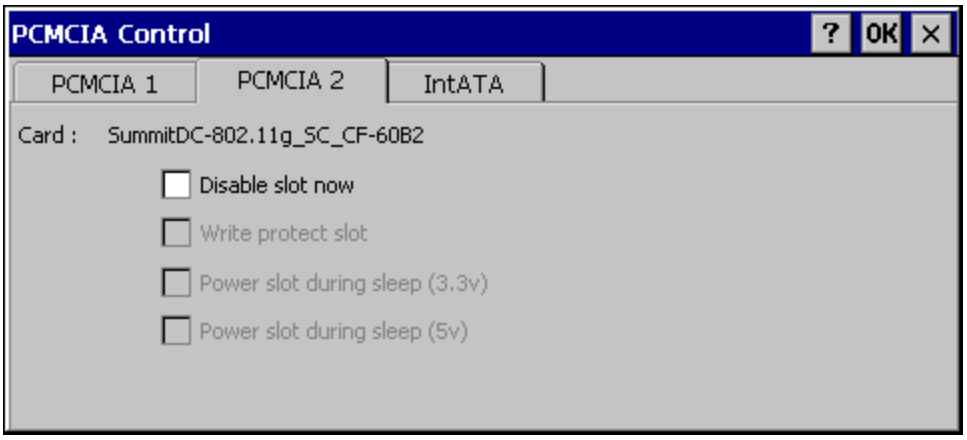
PCMCIA 1



The name of the card (from the CIS data on the card) in the slot is displayed. This information cannot be changed by the user.

When “Disable slot now” is checked, the slot is powered down as soon as the Control Panel is closed and the PCMCIA driver ignores any card in the slot. When there is no card in a slot, the options are dimmed.

PCMCIA 2

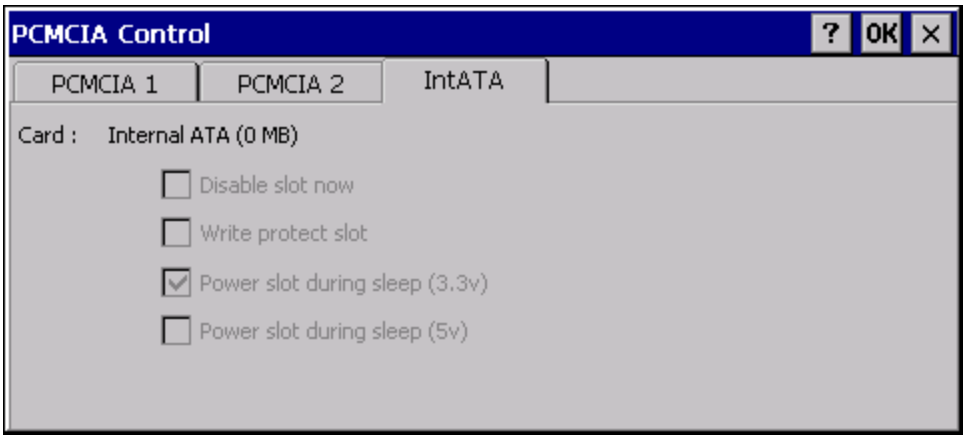


The name of the card (from the CIS data on the card) in the slot is displayed. This information cannot be changed by the user.

When “Disable slot now” is checked, the slot is powered down as soon as the Control Panel is closed and the PCMCIA driver ignores any card in the slot. When there is no card in a slot, the options are dimmed.

IntATA Tab Options

The IntATA Tab provides information on the internal CompactFlash ATA drive. There are no user configurable options.



Power

Start > Settings > Control Panel > Power

The VX7 power mode timers are cumulative.

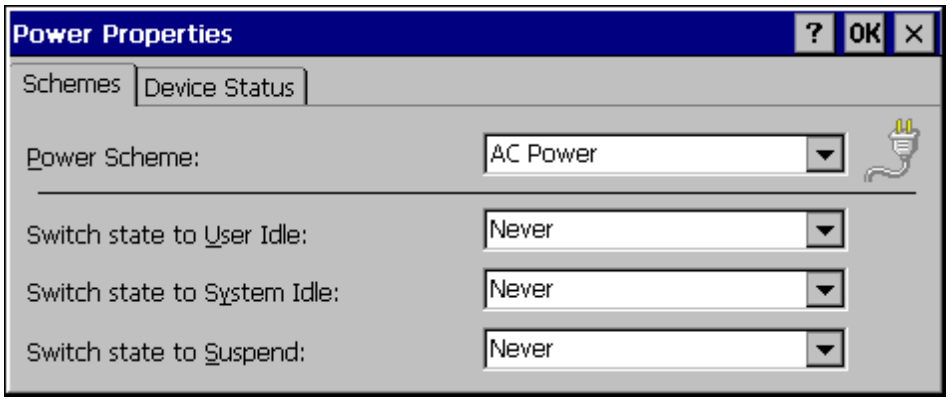
The System Idle timer begins the countdown after the User Idle timer has expired and the Suspend timer begins the countdown after the System Idle timer has expired.

When the User Idle timer is set to “Never”, the power scheme timers never place the device in User Idle, System Idle or Suspend modes (even when the device is idle).

The **Display > Backlight** setting is synchronized with the User Idle setting in the Schemes tab in the Power control panel.

Factory Default Settings

Schemes Tab	
Battery Power - User Idle Timeout	Never
Battery Power - System Idle Timeout	Never
Battery Power - Suspend Timeout	Never
AC Power - User Idle Timeout	Never
AC Power - System Idle Timeout	Never
AC Power - Suspend Timeout	Never
Device Status Tab	No user interaction



Because of the cumulative effect, if the Battery Power Scheme timers are set to 3 seconds, 15 seconds and 5 minutes:

- The backlight turns off after 3 seconds of no activity,
- The display turns off after 18 seconds of no activity (15 sec + 3 sec),
- And the device enters Suspend after 5 minutes and 18 seconds of no activity.
- If the User Idle timer is set to Never, the power scheme timers never place the device in User Idle, System Idle or Suspend modes.

For a VX7, the User Idle state turns off the display backlight. There is no System Idle mode so the VX7 remains in User Idle mode until the Suspend timer expires or a primary event occurs.

The Device Status tab displays the status of power managed devices. Note that since the VX7does not support power management, all devices show the “high” power level. There are no user options on this screen.

As there is no Suspend mode on the VX7. If the Suspend timer is enabled, the VX7 will shut down when the Suspend timer expires.

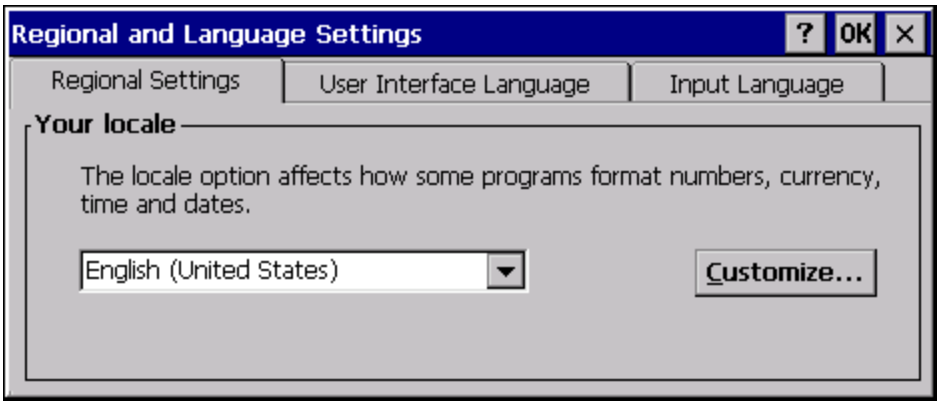
Regional and Language Settings

Start > Settings > Control Panel > Regional Settings

Set the appearance of numbers, currency, time and date based on regional and language settings. Set the VX7 user interface language and the default input language.

Factory Default Settings

Region	
Locale	English (United States)
Number	123,456,789.00 / -123,456,789.00 neg
Currency	$123,456,789.00 pos / ($123,456,789.00) neg
Time	h:mm:ss tt (tt=AM or PM)
Date	M/d/yy short / dddd,MMMM,dd,yyyy long
Language	
User Interface	English (United States)
Input	
Language	English (United States)-US
Installed	English (United States)-US



Regional and Language Settings
?
OK
Regional Settings
User Interface Language
Input Language
User Interface Language
The option will determine the language used for the menus, dialogs and alerts.
English (United States)

Regional and Language Settings
?
OK
Regional Settings
User Interface Language
Input Language
Default Input language
Select the input language to use when you start your device.
English (United States)-US
Installed Input Languages
Select input languages you plan to use.

Remove Programs

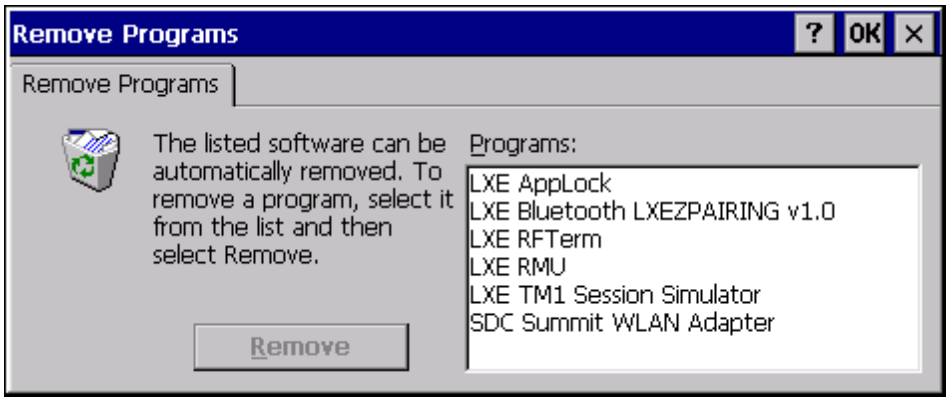
Start > Settings > Control Panel > Remove Programs

Note: Lists programs installed in RAM that have been marked for removal.

In some OS versions, this panel is replaced by Installed Programs.

Select a program and tap Remove. Follow the prompts on the screen to uninstall VX7 user-installed only programs. The change takes effect immediately.

Files stored in the **My Documents** folder are not removed using this option.



Note: Do not remove installed programs using this option. Contact Technical Assistance if installed programs must be deleted.

Scanner

Start > Settings > Control Panel > Scanner

Set VX7 scanner keyboard wedge parameters, enable or disable allowed symbologies, scanner icon appearance, active scanner port, and scan key settings.

Assign baud rate, parity, stop bits and data bits for available COM ports.

Parameters on the Main tab and the COM tab(s) apply to this device only.

Barcode manipulation parameter settings on the Barcode tab are applied to the incoming data resulting from successful barcode scans sent to the VX7 for processing. The successful barcode scan data may be sent by

- a wireless Bluetooth Handheld Scanner,
- or a tethered scanner.

Bar Code Readers

The VX7 can use the following external bar code readers:

- Tethered hand-held scanners are tethered to a serial port on the VX7 and are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.
- Wireless hand-held Bluetooth scanners are configured by scanning the engine-specific bar codes in the scanner manufacturer's programming guide. The manufacturer's guides are usually shipped with the bar code reader.
- The body worn Bluetooth Ring Scanner module may be using a Symbol 4400 Ring Imager or a Symbol 955 Ring Scanner. The BTRS module is configured by scanning the bar codes in the *Bluetooth Ring Scanner Module*.

Return to Factory Default Settings

After scanning the engine-specific bar code to return the scanner/imager to factory default settings, the next step is to open the bar code wedge panel on the mobile device collecting the scanned data. Click the OK button to close the panel. This action will synchronize all scanner formats for your device.

Barcode Processing Overview

Barcode processing involves several steps. Some steps may be skipped during the processing depending on user selections on the Scanner control panels. The steps are presented below in the order they are performed on the barcode data.

1. Scanned barcode is tested for a **code ID** and matching length (Min/Max). If it matches, it is processed per the rules in place for that symbology. If the scan does not meet the criteria for that symbology, it is processed based on the settings for All. If a code ID is not found, the barcode data is processed based on the settings for All.
2. If symbology is **disabled**, the scan is rejected.
3. Strip **leading** data bytes unconditionally.
4. Strip **trailing** data bytes unconditionally.
5. Parse for, and strip if found, **Barcode Data** strings.
6. Replace any **control characters** with string, as configured.
7. Add **prefix** string to output buffer.
8. If **Code ID** is ***not*** stripped, add saved **code ID** from above to output buffer.

9. Add processed **barcode string** from above to output buffer.
10. Add **suffix string** to output buffer.
11. Add a terminating **NUL** to the output buffer, in case the data is processed as a string.
12. If key output is enabled, start the process to output keys. If control characters are encountered:

    - If Translate All is set, key is translated to CTRL + char, and output.
    - If Translate All is not set, and key has a valid VK code, key is output.
    - Otherwise, key is ignored (not output).

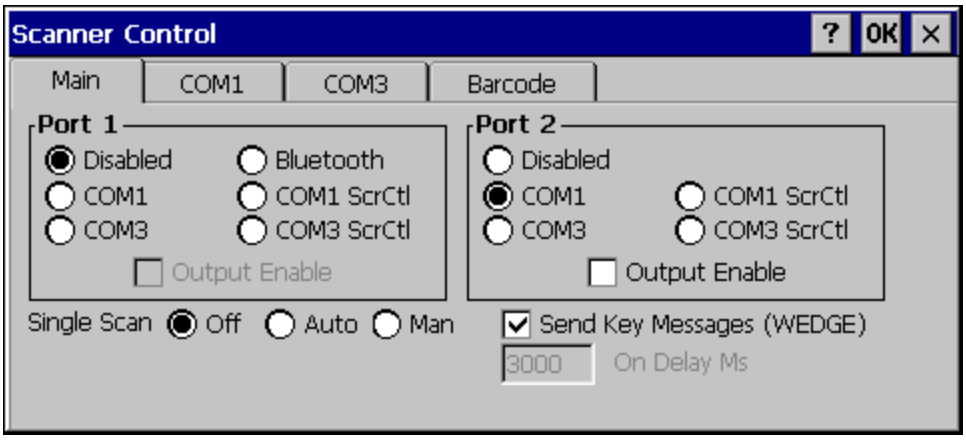
The barcode data is ready to be read by applications.

Factory Default Settings

Main Tab	
Port 1	Disabled
Port 2	COM1
Send Key Message (WEDGE)	Enabled
Single Scan	Off
On Delay MS	3000
COM Ports (COM1,COM3)	
Baud Rate	9600
Stop Bits	1
Parity	None
Data Bits	8
Power on Pin 9	COM1: On COM3: Off
Enable handshaking	Disabled
Barcode Tab	
Enable Code ID	None

Main Tab

Start > Settings > Control Panel > Scanner > Main tab



Parameter	Function
Port	Default: Port 1 is disabled. Port 2 COM1 is enabled. COM1 ScrCtl and COM3 ScrCtl are used to enable the screen blanking function.
Send Key Messages (WEDGE)	Default: Enabled. If “Send Key Messages (WEDGE)” is checked, the Scanner Driver is in “Key Message” (also known as “character”) mode which sends the bar codes to the application with the focus as keystrokes. All data scanned is converted to keystrokes and sent to the active window. If “Send Key Messages (WEDGE)” is not checked, the Scanner Driver is in “Block” mode which buffers the data that can be read by an application from the WDG: device through the OS or APIs. Note that this latter method is significantly faster than using “Wedge”. Even if Send Key Messages is enabled (“key mode”), the data is still available using the scanner APIs (“block mode”). If two or more applications are reading the data in Block mode, ClearBuf must be set to Off so data is not erased when read. Please refer to the CE API Programming Guide for details on scanner APIs.
Single Scan	Single Scan determines if scanner input is inhibited after a scan until the scanner is re-enabled. Off - Single Scan mode is off. Auto - Single Scan mode is on. The scanner is disabled after a scan and automatically re-enabled by the scanner driver after retrieving the bar code data. Man - Single Scan mode is on. The scanner is disabled after a scan and the user application must call LXEScannerSSReset to re-enable the scanner. See the CE API Programming Guide for more details. This option is only supported on Symbol Motorola) internal and BTRS scanners. The scanner may require a firmware upgrade to support this feature. Contact Technical Assistance for details.
On Delay Ms	Specifies the delay for the screen blanking function before turning on the display.

Click here to view factory default settings for this panel.

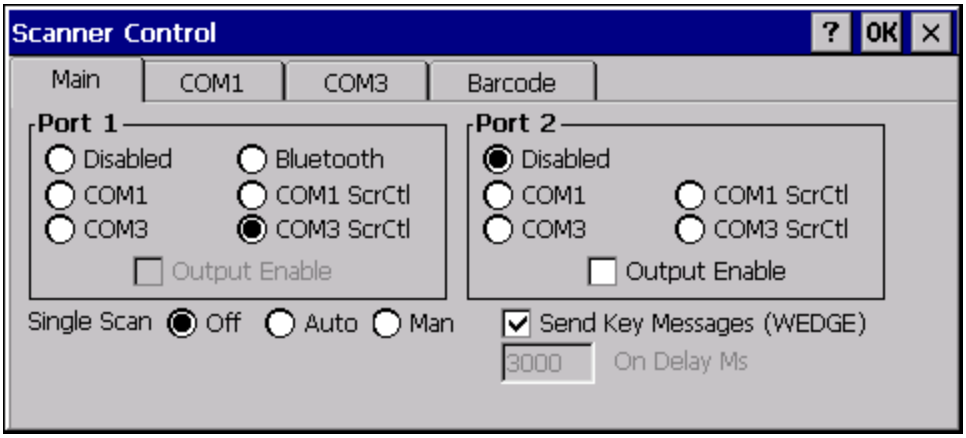
Screen Blanking

The VX7 can be configured to blank the display when the vehicle to which it is mounted is moving, eliminating a possible distraction for the driver. When configured properly, the screen blanking feature provides a tamper resistant method to blank the vehicle screen. The screen blanking feature consists of Scanner Control Panel Options and a customer supplied cable connected to one of the COM ports on the VX7. Properly configured, the display is visible only when the cable provides a signal that the vehicle has stopped.

The customer must supply their own cable. The cable specifications are detailed in "Technical Specifications – Screen Blanking Cable".

The cable can be hooked to either the COM1 or COM3 port. The COM port used must be selected in the **Scanner** control panel.

Screen blanking is configured on the **Main** tab of the **Scanner** control panel.



- If the COM1/COM3 screen blanking and On Delay choices are not shown, the system load must be updated.
- Warning: Do not select **COM1 ScrCtl** or **COM3 ScrCtl** unless you have already attached the cable. Failure to attach the cable before selecting a screen blanking option will cause the screen to go blank (and remain blank) until an appropriate cable is attached to the specified COM port.

Set the desired COM port (COM1 ScrCtl or COM3 ScrCtl) and On Delay. Press **OK**. The On Delay can be used to specify the time (in milliseconds) before the display turns on. For example, use the On Delay if the switch end of the cable is attached to the vehicle's accelerator pedal. Release of the accelerator may mean the truck is coasting to a stop rather than stationary. Configure the delay to allow time for the vehicle to coast to a stop.

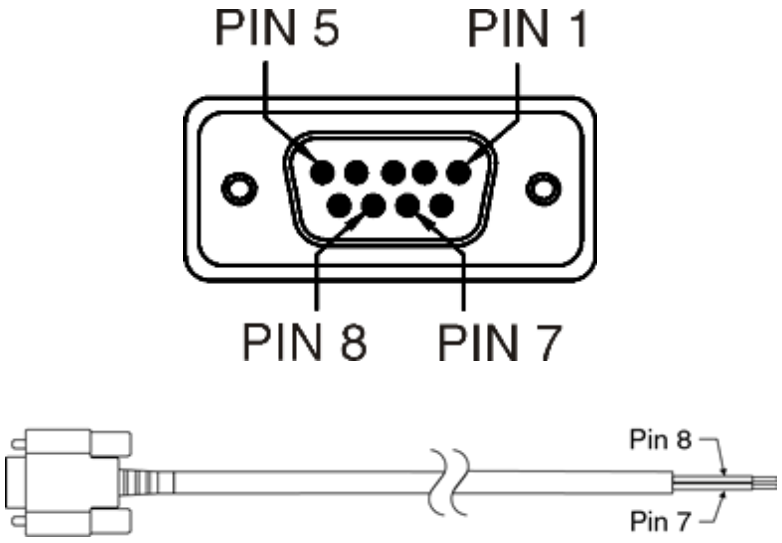
To disable screen blanking, select COM1 or COM3 to return the selected COM port to normal operation.

Technical Specifications - Screen Blanking Cable

The customer must supply their own cable. The cable must be designed so that pin 7 (RTS – Request to Send Output) and pin 8 (Clear to Send Input) of a DB9 female connector provide continuity only when the vehicle is stopped (for example, via a switch on the accelerator pedal of the fork truck). All other pins on the connector must be left unconnected. If pins 7 and 8 do not provide continuity (or the cable is removed), the VX7 screen remains blank.

Serial cable

Customer built cable with the following specifications:

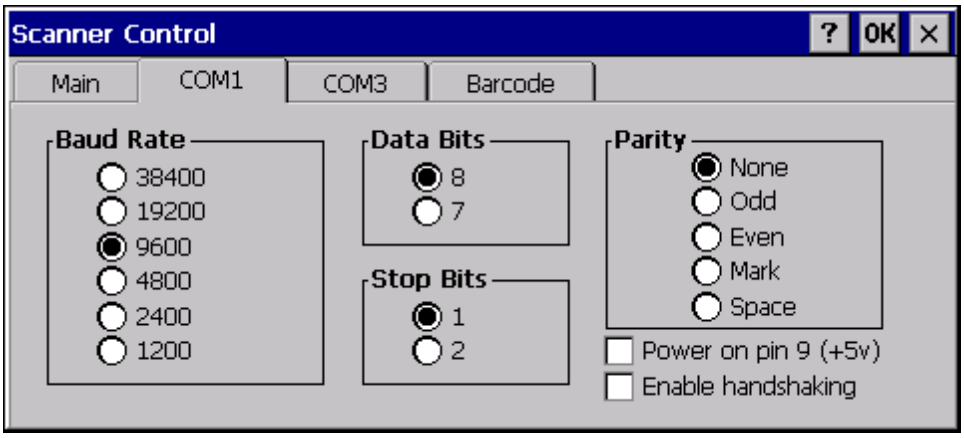


Pinout

DB9 Female	Function
1	Not Used
2	Not Used
3	Not Used
4	Not Used
5	Not Used
6	Not Used
7 (RTS)	No signal when in motion. Continuity to Pin 8 when vehicle stopped.
8 (CTS)	No signal when in motion. Continuity to Pin 7 when vehicle stopped.
9	Not Used

COM1 Tab

Start > Settings > Control Panel > Scanner > COM1



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

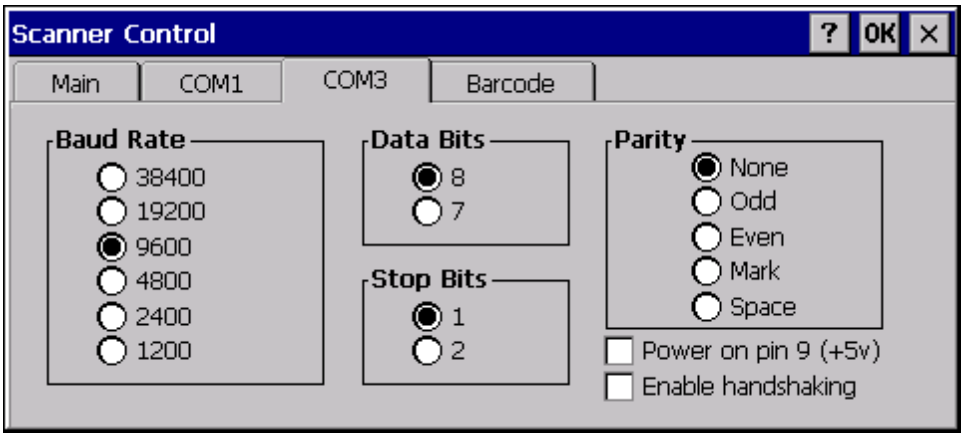
This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Click here to set Power on Pin 9

Click here to Enable Handshaking

COM3 Tab

Start > Settings > Control Panel > Scanner > COM3



This panel sets communication parameters for any device connected to the external port.

Adjust the settings and click the OK button to save the changes. Any changes take effect immediately.

This panel does not configure the connected device. Please refer to the documentation for the external connected or wireless device for information on configuring the device.

Click here to set Power on Pin 9

Click here to Enable Handshaking

Serial Port Pin 9

To configure the COM port to supply power to an external scanner tethered to the COM port, check the checkbox for Power on Pin 9 (+5V). The external scanner is powered by the VX7's power source. Wireless external scanners use their own power source.

To configure a COM port for Ring Indicator (RI) on Pin 9, uncheck the checkbox for Power on Pin 9 (+5V) (disabled).

The default is On (+ 5V enabled) for COM1, Off (RI enabled) for COM3.

Enable Handshaking

To enable handshaking on the indicated serial port, check the Enable handshaking box.

The default is disabled (unchecked)

Barcode Tab

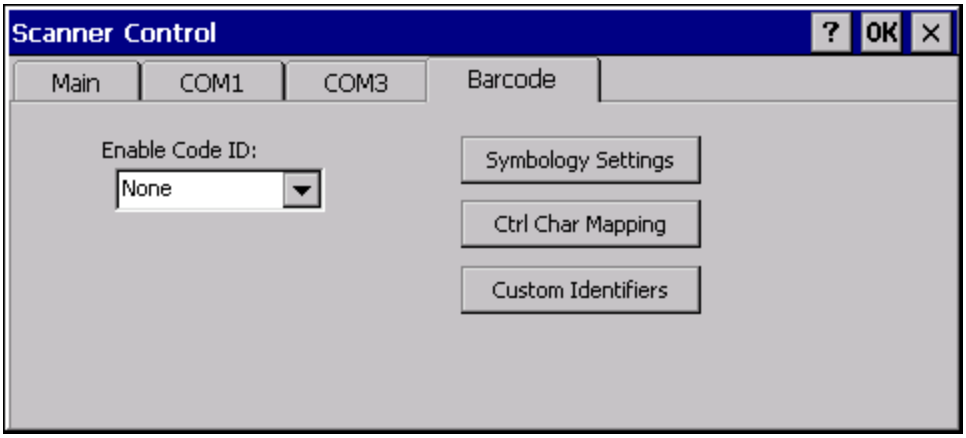
Start > Settings > Control Panel > Scanner > Barcode tab

The Barcode tab contains several options to control barcode processing. Options include:

- Defining custom Code IDs
- Disable processing of specified barcode symbologies
- Rejecting barcode data that is too short or too long
- Stripping characters including Code ID, leading or trailing characters and specified barcode data strings
- Replacing control characters
- Adding a prefix and a suffix.

Notes:

- The Scanner application (Wedge) can only enable or disable barcode processing inside the Wedge software.
- The Scanner application enables or disables the Code ID that may be scanned.
- Enabling or disabling a specific barcode symbology is done manually using the configuration barcode. Configuration barcodes for external scanner are available in the manual provided with the scanner.



Choose an option in the Enable Code ID drop-down box: None or Custom ID.

Buttons

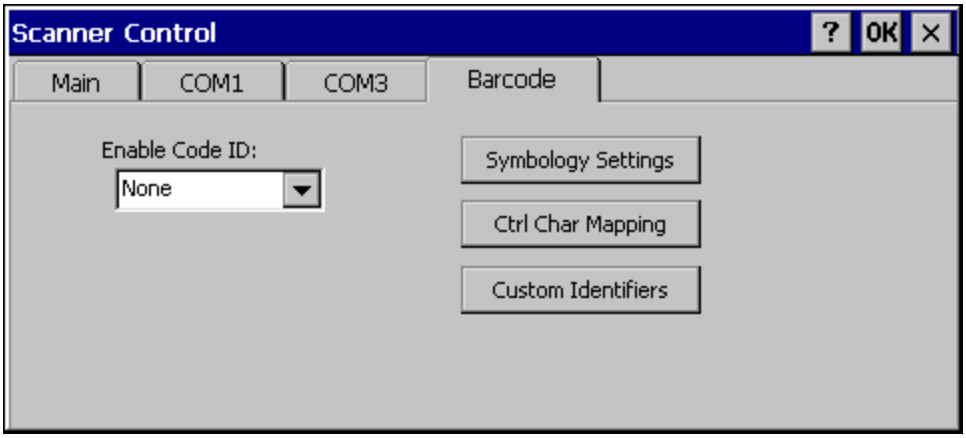
Symbology Settings	Individually enable or disable a barcode from being scanned, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode before transmission.
Ctrl Char Mapping	Define the operations the Wedge performs on control characters (values less than 0x20) embedded in barcodes.
Custom Identifiers	Defines an identifier that is at the beginning of barcode data which acts as a Code ID. After a Custom Identifier is defined, Symbology Settings can be defined for the identifier.

See "Barcode Processing Overview".

Enable Code ID

This parameter programs the scanner to transmit the specified Code ID and/or determines the type of barcode identifier being processed.

Transmission of the Code ID is enabled at the scanner for all barcode symbologies, not for an individual symbology. Code ID is sent from the scanner so the scanner driver can discriminate between symbologies.



Options

- **None:** Programs an internal scanner to disable transmission of a code ID. After clicking the Symbology Settings button, the only entry on the Symbology listing is All, plus any configured custom IDs. Select this option to disable Code ID processing. The barcode data is received, but is not checked for a Code ID.
- **Custom:** Does not change the internal scanner's Code ID transmission setting. After clicking the Symbology Settings button, the Symbology listing includes all Custom Code IDs. Select this option to enable processing of barcodes with a custom Code ID.

Notes

- When Strip: Code ID (see Symbology panel) is not enabled, the code ID is sent as part of the barcode data to an application.
- When Strip: Code ID (see Symbology panel) is enabled, the entire Code ID string is stripped (i.e. treated as a Code ID).
- **UPC/EAN Codes only**: The code id for supplemental barcodes is not stripped.
- When Enable Code ID is set to **None**, Code IDs are ignored.
- Custom symbologies appear at the end of the list in the Symbology dialog, but will be processed at the beginning of the list in the scanner driver. This allows custom IDs, based on actual code IDs, to be processed before the Code ID.
- When using the parameters in the Scanner Control Panel to manage indicators for good read/bad read decoding, the number or patterns of beeps heard may be confusing. Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from an external scanner triggers a good scan beep, and then the rejection of scanned barcode data by the Scanner Control Panel processing causes a bad scan beep by the mobile device on the same data.

Barcode – Custom Identifiers

Code IDs can be defined by the user. This allows processing parameters to be configured for barcodes that do not use the standard IDs or for barcodes that have data embedded at the beginning of the data that acts like a Code ID.

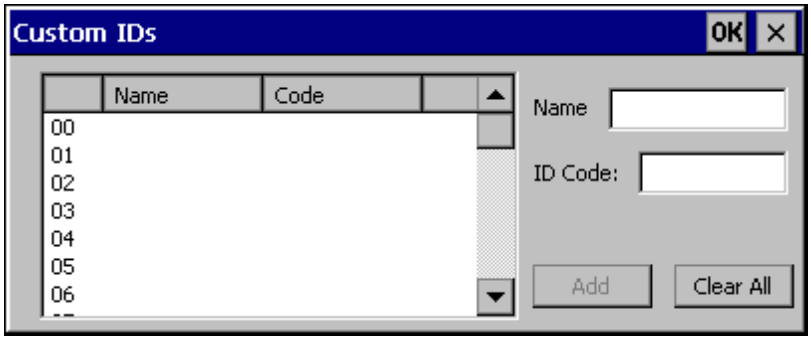
These are called **custom Code ID**s and are included in the Symbology drop down box in the Symbology dialog, unless **Enable Code ID** is set to **None**. When the custom Code ID is found in a barcode, the configuration specified for the custom Code ID is applied to the barcode data.

When **Enable Code ID** is set to **None**, custom code IDs are ignored.

Note: Custom symbologies will appear at the end of the list in the Symbology dialog, and are processed at the beginning of the list in the scanner driver itself. This allows custom IDs based on actual code IDs to be processed before the code ID itself.

*Note: When **Strip: Code ID** is enabled, the entire custom Code ID string is stripped (i.e., treated as a Code ID).*

The dialog box shown below allows the custom Code IDs to be configured. When incoming data is checked for a custom ID code, the list is compared in the order displayed in this dialog box.



After adding, changing and removing items from the Custom IDs list, click the OK button to save changes and return to the Barcode panel.

Parameters

Name text box

Name is the descriptor that is used to identify the custom Code ID. Names must be unique from each other; however, the Name and ID Code may have the same value. Name is used in the Symbology drop down box to identify the custom Code ID in a user-friendly manner. Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

ID Code text box

ID Code defines the data at the beginning of a barcode that acts as an identifier (the actual Code ID). Both Name and ID Code must be specified in order to add a custom Code ID to the Custom IDs list.

Buttons

Add

Entering data into both the Name and ID Code fields enables the Add button. Click the Add button and the data is added to the next empty location in the Custom ID list.

Insert

Click on an empty line in the Custom ID list. The Add button changes to Insert. Enter data into both the Name and ID Code fields and click the Insert button. The data is added to the selected line in the Custom IDs list.

Edit

Double click on the item to edit. Its values are copied to the text boxes for editing. The Add button changes to Replace. When Replace is clicked, the values for the current item in the list are updated.

Clear All

When no item in the Custom IDs list is selected, clicking the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.

Remove

The Clear All button text changes to a Remove button when an item in the Custom IDs list is selected. Click the desired line item and then click the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Control Code Replacement Examples

Configuration Data	Translation	Example Control Character	Example Configuration	Translated Data
Ignore (drop)	The control character is discarded from the barcode data, prefix and suffix	ESCape	Ignore (drop)	0x1B in the barcode is discarded.
Printable text	Text is substituted for Control Character.	Start of TeXt	STX	0x02 in a barcode is converted to the text STX.
Hat-encoded text	The hat-encoded text is translated to the equivalent hex value.	Carriage Return	^M	Value 0x0d in a barcode is converted to the value 0x0d.
Escaped hat-encoded text	The hat-encoding to pass through to the application.	Horizontal Tab	\^I	Value 0x09 in a barcode is converted to the text ^I.
Hex-encoded text	The hex-encoded text is translated to the equivalent hex value.	Carriage Return	0x0A	Value 0x0D in a barcode is converted to a value 0x0A.
Escaped hex-encoded text	The hex-encoding to pass through to the application.	Vertical Tab	\0x0A or 0\x0A	Value 0x0C is a barcode is converted to text 0x0A

See Also: "Hat Encoding"

Barcode Processing Examples

The following table shows examples of stripping and prefix/suffix configurations. The examples assume that the scanner is configured to transmit a Code ID and the proper Custom IDs have been configured.

	Symbology				
	All	**EAN-128(]C1)**	**EAN-13(]E0)**	**Intrlv 2 of 5(]I0)**	**Code93**
Enable	Enabled	Enabled	Enabled	Enabled	Disabled
Min length	1	4	1	1	
Max length	all	all	all	10	
Strip Code ID	Enabled	Enabled	Disabled	Enabled	
Strip Leading	3	0	3	3	
Strip Barcode Data		*123	1*	456	
Strip Trailing	0	0	3	3	
Prefix	aaa	bbb	ccc	ddd	
Suffix	www	xxx	yyy	zzz	

Provided that the wedge is configured with the above table, below are examples of scanned barcode data and results of these manipulations.

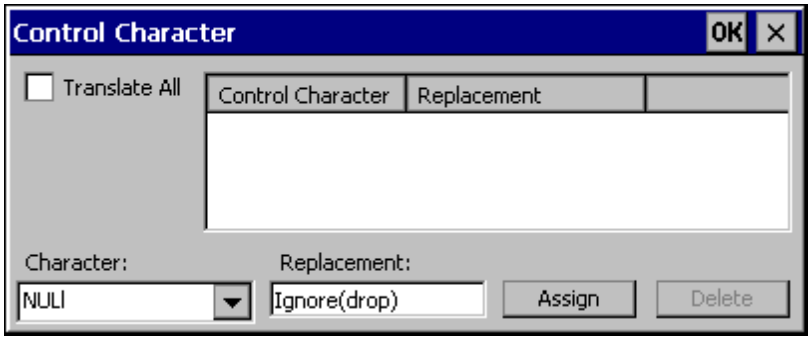
Barcode Symbology	**Raw Scanner Data**	**Resulting Data**
EAN-128	]C11234567890123	bbb1234567890xxx
EAN-128	]C111234567890123	bbb11234567890xxx
EAN-128	]C1123	*< rejected > (too short)*
EAN-13	]E01234567890987	ccc]E04567890yyy
EAN-13	]E01231234567890987	ccc]E0234567890yyy
EAN-13	]E01234	ccc]E0yyy
I2/5	]I04444567890987654321	***< rejected >*** *(too long)*
I2/5	]I04444567890123	ddd7890zzz
I2/5	]I0444	dddzzz
I2/5	]I022245622	ddd45zzz
Code-93	]G0123456	***< rejected >*** *(disabled)*
Code-93	]G0444444	***< rejected >*** *(disabled)*
Code-39	]A01234567890	aaa4567890www
Code-39 full ASCII	]A41231234567890	aaa1234567890www
Code-39	]A4	***< rejected >*** *(too short)*

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep (from the external scanner), and then the rejection of scanned barcode data by the processing causes a bad scan beep on the same data.

Barcode - Ctrl Char Mapping

The Ctrl Char Mapping button (Control Character Mapping) activates a dialog to define the operations the Wedge performs on control characters (values less than 0x20) embedded in barcodes. Control characters can be replaced with user-defined text which can include hat encoded or hex encoded values.

In key message mode, control characters can also be translated to their control code equivalent key sequences.



Translate All

When **Translate All is checked**, unprintable ASCII characters (characters below 20H) in scanned barcodes are assigned to their appropriate CTRL code sequence when the barcodes are sent in Character mode.

The wedge provides a one-to-one mapping of control characters to their equivalent control+character sequence of keystrokes. If control characters are translated, the translation is performed on the barcode data, prefix, and suffix before the keystrokes are simulated.

Parameters

Translate All

This option is grayed unless the user has Send Key Messages (WEDGE) on the Main tab selected.

In Key Message mode, when this option is enabled, control characters embedded in a scanned barcode are translated to their equivalent control key keystroke sequence (13 [0x0d] is translated to Control+M keystrokes as if the user pressed the CTRL, SHIFT, and m keys on the keypad).

Additionally, when Translate All is disabled, any control code which has a keystroke equivalent (enter, tab, escape, backspace, etc.) is output as a keystroke.

Any control code without a keystroke equivalent is dropped.

Character

This is a drop down combo box that contains the control character name. Refer to the Character drop down box for the list of control characters and their names.

When a character name is selected from the drop down box, the default text *Ignore (drop)* is shown and highlighted in the Replacement edit control. *Ignore (drop)* is highlighted so the user can type a replacement if the control character is not to be ignored.

Once the user types any character into the Replacement edit control, reselecting the character from the Character drop down box redisplays the default *Ignore (drop)* in the Replacement edit control.

Replacement

The edit control where the user types the characters to be assigned as the replacement of the control character.

Replacements for a control character are assigned by selecting the appropriate character from the Character drop down box, typing the replacement in the Replacement edit control (according to the formats defined above) and then clicking the button. The assigned replacement is then added to the list box above the Assign button.

For example, if Carriage Return is replaced by Line Feed (by specifying ^J or 0x0A) in the configuration, the value 0x0d received in any scanned barcode (or defined in the prefix or suffix) will be replaced with the value 0x0a.

The Wedge then sends Ctrl+J to the receiving application, rather than Ctrl+M.

List Box

The list box shows all user-defined control characters and their assigned replacements.

All replacements are enclosed in single quotes to delimit white space that has been assigned.

Assign Button

Click this button when you want to assign the characters in the Replacement text box to the character in the Character drop down box.

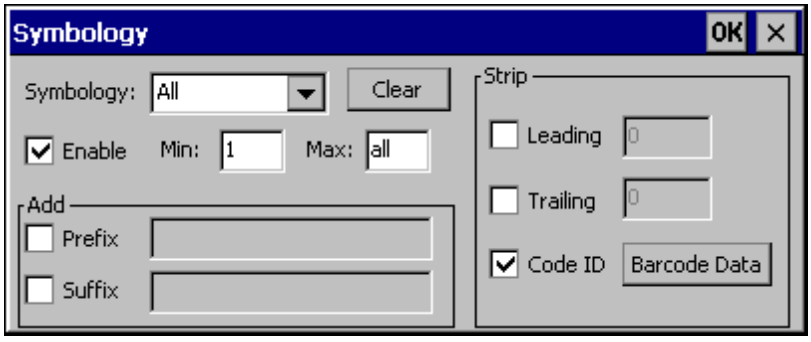
Delete Button

This button is grayed unless an entry in the list box is highlighted.

When an entry (or entries) is highlighted, and the Delete button is clicked, the highlighted material is deleted from the list box.

Barcode - Symbology Settings

The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured. The features available on the Symbology Settings dialog include the ability to individually enable or disable a barcode from scanning, set the minimum and maximum size barcode to accept, strip Code ID, strip data from the beginning or end of a barcode, or (based on configurable Barcode Data) add a prefix or suffix to a barcode.



The Symbology drop-down box contains all custom symbologies **the user has defined on the VX7**. An asterisk appears in front of symbologies that have already been configured or have been modified from the default value.

Each time a Symbology is changed, the settings are saved as soon as the OK button is clicked. Settings are also saved when a new Symbology is selected from the Symbology drop-down list.

Clear Button -- Clicking this button will erase any programmed overrides, returning to the default settings for the selected symbology. If **Clear** is pressed when **All** is selected as the symbology, a confirmation dialog appears, then all symbologies are reset to their factory defaults, and all star (*) indications are removed from the list of Symbologies.

The order in which these settings are processed are:

- Min / Max
- Code ID
- Leading / Trailing
- Barcode Data
- Prefix / Suffix

*Note: When **Enable Code ID** is set to **None** on the Barcode tab and when **All** is selected in the Symbology field, **Enable** and **Strip Code ID** on the Symbology panel are grayed and the user is not allowed to change them, to prevent deactivating the scanner completely.*

When **All** is selected in the Symbology field and the settings are changed, the settings in this dialog become the defaults, used unless overwritten by the settings for individual symbologies. This is also true for Custom IDs, where the code IDs to be stripped are specified by the user.

*Note: In Custom mode on the Barcode tab, any Code IDs **not** specified by the user will not be stripped, because they will not be recognized as Code IDs.*

If a specific symbology's settings have been configured, a star (*) will appear next to it in the Symbology drop-down box, so the user can tell which symbologies have been modified from their defaults.

If a particular symbology has been configured, the entire set of parameters from that symbologies screen are in effect for that symbology. In other words, either the settings for the configured symbology will be used, or the default settings are used, not a combination of the two.

If a symbology has not been configured (does not have an * next to it) the settings for **All** are used which is not necessarily the default.

Parameters

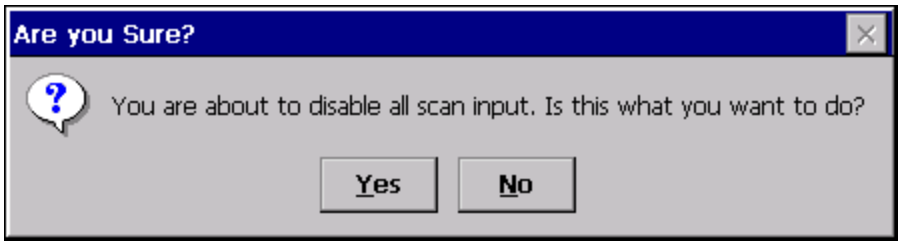
Enable

This checkbox enables (checked) or disables (unchecked) the symbology field.

The scanner driver searches the beginning of the barcode data for the type of ID specified in the Barcode tab -- Enable Code ID field plus any custom identifiers.

When a code ID match is found as the scanner driver processes incoming barcode data, if the symbology is disabled, the barcode is rejected. Otherwise, the other settings in the dialog are applied and the barcode is processed. If the symbology is disabled, all other fields on this dialog are grayed.

When there are ***no** customized symbology settings*, and the Enable checkbox is unchecked, while All is selected, a warning message is displayed.



Click the Yes button or the No button. Click the X button to close the dialog without making a decision.

If there ***are** customized settings*, uncheck the Enable checkbox for the All symbology. This results in disabling all symbologies *except* the customized ones.

Min

This field specifies the minimum length that the barcode data (not including Code ID) must meet to be processed.

Any barcode scanned that is less than the number of characters specified in the Min field is rejected. The default for this field is 1.

Max

This field specifies the maximum length that the barcode data (not including Code ID) can be processed. Any barcode scanned that has more characters than specified in the Max field is rejected. The default for this field is All (9999).

If the value entered is greater than the maximum value allowed for that symbology, the maximum valid length is used instead.

Strip Leading/Trailing Control

This group of controls determines what data is removed from the barcode before the data is buffered for the application. When all values are set, Code ID takes precedence over Leading and Trailing; Barcode Data stripping is performed last. Stripping occurs before the Prefix and Suffix are added, so does not affect them.

If the total number of characters being stripped is greater than the number of characters in the barcode data, it becomes a zero byte data string. If, in addition, Strip Code ID is enabled, and no prefix or suffix is configured, the processing will return a zero-byte data packet, which will be rejected.

The operation of each type of stripping is defined below:

Leading

This strips the number of characters specified from the beginning of the barcode data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Trailing

This strips the number of characters specified from the end of the barcode data (not including Code ID). The data is stripped unconditionally. This action is disabled by default.

Code ID

Strips the Code ID based on the type code id specified in the Enable Code ID field in the Barcode tab. By default, Code ID stripping is enabled for all symbologies (meaning code IDs will be stripped, unless specifically configured otherwise).

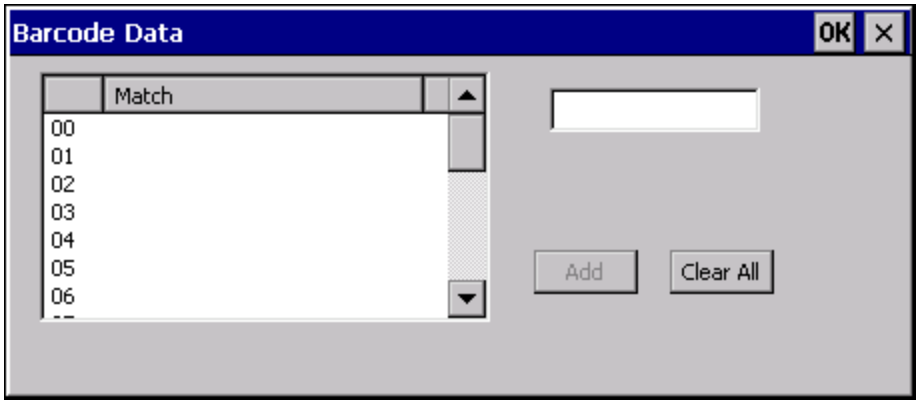
Barcode Data Match List

Barcode Data Panel

This panel is used to strip data that matches the entry in the Match list from the barcode. Enter the data to be stripped in the text box and tap the Insert or Add button. The entry is added to the Match list.

To remove an entry from the Match list, highlight the entry in the list and tap the Remove button.

Tap the OK button to store any additions, deletions or changes.



Barcode Data Match Edit Buttons

Add	Entering data into the text entry box enables the Add button. Tap the **Add** button and the data is added to the next empty location in the Custom ID list.
Insert	Tap on an empty line in the Custom ID list. The **Add** button changes to **Insert**. Enter data into both the Name and ID Code fields and tap the Insert button. The data is added to the selected line in the Custom IDs list.
Edit	Double tap on the item to edit. Its values are copied to the text boxes for editing. The **Add** button changes to **Replace**. When Replace is tapped, the values for the current item in the list are updated.
Clear All	When no item in the Custom IDs list is selected, tapping the Clear All button clears the Custom ID list and any text written (and not yet added or inserted) in the Name and ID Code text boxes.
Remove	The **Clear All** button changes to a **Remove** button when an item in the Custom IDs list is selected. Tap the desired line item and then tap the Remove button to delete it. Line items are Removed one at a time. Contents of the text box fields are cleared at the same time.

Notes

- **Prefix** and **Suffix** data is always added on after stripping is complete, and is not affected by any stripping settings.
- If the stripping configuration results in a 0 length barcode, a good beep will still be sounded, since barcode data was read from the scanner.

Match List Rules

The data in the match list is processed by the rules listed below:

- Strings in the list will be searched in the order they appear in the list. If the list contains ***ABC*** and ***AB***, in that order, incoming data with ***ABC*** will match first, and the ***AB*** will have no effect.
- When a match between the first characters of the barcode and a string from the list is found, that string is stripped from the barcode data.
- Processing the list terminates when a match is found or when the end of the list is reached.
- If the wildcard * is not specified, the string is assumed to strip from the beginning of the barcode data. The string ***ABC**** strips off the prefix ***ABC***. The string ****XYZ*** will strip off the suffix ***XYZ***. The string ***ABC*XYZ*** will strip both prefix and suffix together. More than one * in a configuration string is not allowed. (The User Interface will not prevent it, but results would not be as expected, as only the first * is used in parsing to match the string.)

- The question mark wildcard **?** may be used to match any single character in the incoming data. For example, the data AB?D will match ABCD, ABcD, or AB0D, but not ABDE.
- The Barcode Data is saved per symbology configured. The Symbology selected in the Symbologies dialog defines the symbology for which the data is being configured.
- Note that the Code ID (if any are configured) is ignored by this dialog, regardless of the setting of **Strip: Code ID** in the Symbologies dialog. According to the sequence of events (specified above), the Code ID must not be included in the barcode data being matched, because when the matching test occurs, the Code ID has already been stripped. If Strip Code ID is disabled, then the barcode data to match must include the Code ID. If Strip Code ID is enabled, the data should not include the Code ID since it has already been stripped.

Add Prefix/Suffix Control

Use this option to specify a string of text, hex values or hat encoded values to be added to the beginning (prefix) or the end (suffix) of the barcode data. Up to 19 characters can be included in the string. The string can include any character from the keyboard plus characters specified by hex equivalent or entering in hat encoding. Please see Hat Encoding for a list of characters with their hex and hat-encoded values.

Using the Escape function allows entering of literal hex and hat values.

Add Prefix	To enable a prefix, check the Prefix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Prefix string is sent to the output buffer before any other data. Because all stripping operations have already occurred, stripping settings do not affect the prefix. The prefix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the prefix is added for any symbology that has not been specifically configured.
Add Suffix	To enable a suffix, check the Suffix checkbox and enter the desired string in the textbox. The default is disabled (unchecked) with a blank text string. When barcode data is processed, the Suffix string is sent to the output buffer after the barcode data. Because all stripping operations have already occurred, stripping settings do not affect the suffix. The suffix is added to the output buffer for the Symbology selected from the pull down list. If 'All' is selected, the suffix is added for any symbology that has not been specifically configured.

Note: Non-ASCII equivalent keys in Key Message mode are unavailable in this option. Non-ASCII equivalent keys include the function keys (e.g. F1), arrow keys, Page up, Page down, Home, and End.

Length Based Barcode Stripping

Use this procedure to create symbology rules for two barcodes with the same symbology but with different discrete lengths. This procedure is not applicable for barcodes with variable lengths (falling between a maximum value and a minimum value).

Example:

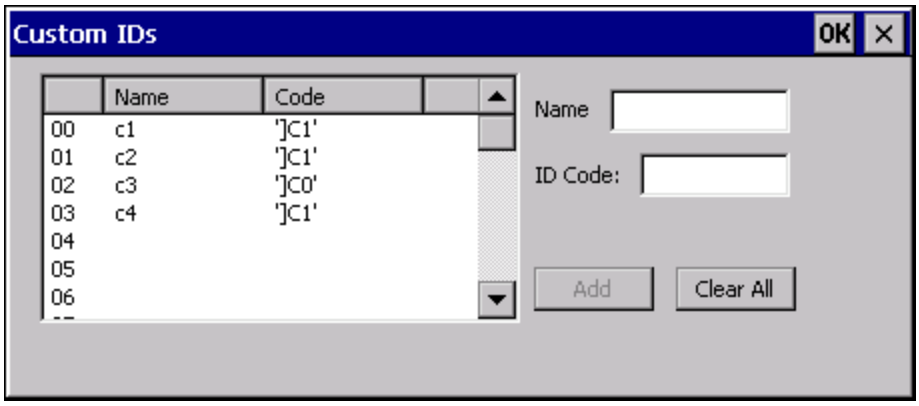
For the purposes of this example, the following sample barcode parameters will be used – EAN 128 and Code 128 barcodes. Some of the barcodes start with '00' and some start with '01'. The barcodes are different lengths.

- 34 character length with first two characters = “01” (strip first 2 and last 18)
- 26 character length with first two characters = “01” (strip first 2 and last 10)
- 24 character length with first two characters = “01” (strip first 2 and last 8). This 24 character barcode is Code 128.
- 20 character length with first two characters = “00” (strip first 0 (no characters) and last 4)

On the Barcode tab, set Enable Code ID to Custom.

Create four custom IDs, using 1 for EAN 128 barcode and 0 for Code 128 barcode.

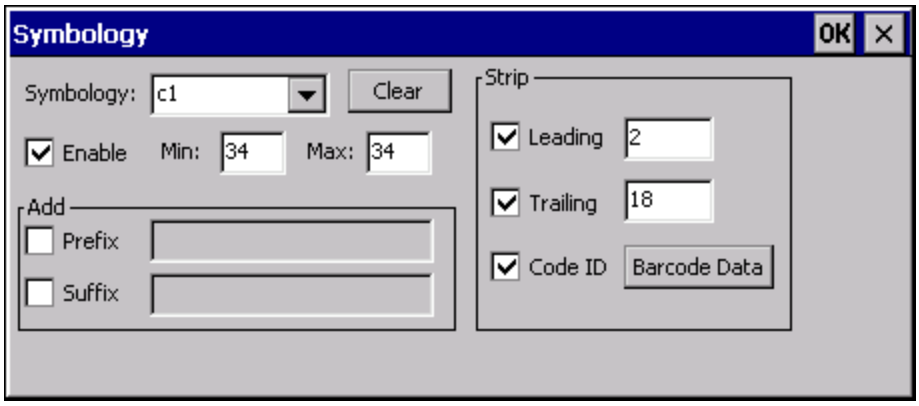
- c1 = Code = ‘]C1’
- c2 = Code = ‘]C1’
- c3 = Code = ‘]C0’ (24 character barcode is Code 128)
- c4 = Code = ‘]C1’



Custom symbology setup is assigned in the following manner:

- c1 min length = 34, max length = 34, strip leading 2, strip trailing 18, Code ID enabled, Barcode Data = “01”
- c2 min length = 26, max length = 26, strip leading 2, strip trailing 10, Code ID enabled, Barcode Data = “01”
- c3 min length = 24, max length = 24, strip leading 2, strip trailing 8, Code ID enabled, Barcode Data = “01”
- c4 min length = 20, max length = 20, strip leading 0, strip trailing 4, Code ID enabled, Barcode Data = “00”

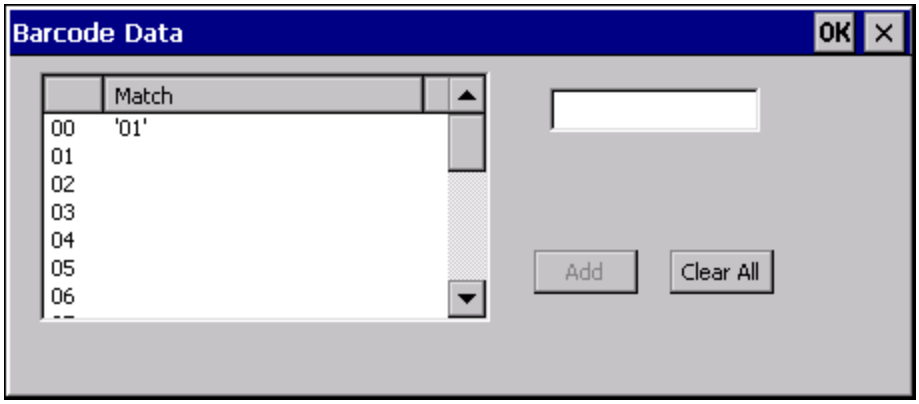
Add the custom symbologies. Refer to the previous section *Barcode – Symbology Settings* for instruction.



Click the Barcode Data button.

Click the Add button.

Add the data for the match codes.



Refer to the previous section Barcode Data Match List for instruction.

Scan a barcode and examine the result.

Hat Encoding

Desired ASCII	Hex Value	Hat Encoded
NUL	0X00	^@
SOH	0X01	^A
STX	0X02	^B
ETX	0X03	^C
EOT	0X04	^D
ENQ	0X05	^E
ACK	0X06	^F
BEL	0X07	^G
BS	0X08	^H
HT	0X09	^I
LF	0X0A	^J
VT	0X0B	^K
FF	0X0C	^L
CR	0X0D	^M
SO	0X0E	^N
SI	0X0F	^O
DLE	0X10	^P
DC1 (XON)	0X11	^Q
DC2	0X12	^R
DC3 (XOFF)	0X13	^S
DC4	0X14	^T
NAK	0X15	^U
SYN	0X16	^V
ETB	0X17	^W
CAN	0X18	^X
EM	0X19	^Y
SUB	0X1A	^Z
ESC	0X1B	^[
FS	0X1C	^\\
GS	0X1D	^]
RS	0X1E	^^
US	0X1F	^ (Underscore)
	0X7F	^?
	80	~^@
	81	~^A
	82	~^B
	83	~^C
IND	84	~^D
NEL	85	~^E
SSA	86	~^F
®	AE	~. (Period)
¯	AF	~/
°	B0	~0 (Zero)
±	B1	~1

Desired ASCII	Hex Value	Hat Encoded
ESA	87	~^G
HTS	88	~^H
HTJ	89	~^I
VTS	8A	~^J
PLD	8B	~^K
PLU	8C	~^L
RI	8D	~^M
SS2	8E	~^N
SS3	8F	~^O
DCS	90	~^P
PU1	91	~^Q
PU2	92	~^R
STS	93	~^S
CCH	94	~^T
MW	95	~^U
SPA	96	~^V
EPA	97	~^W
	98	~^X
	99	~^Y
	9A	~^Z
CSI	9B	~^[
ST	9C	~^\\
OSC	9D	~^]
PM	9E	~^^
APC	9F	~^_ (Underscore)
(no-break space)	A0	~ (Tilde and Space)
¡	A1	~!
¢	A2	~"
£	A3	~#
¤	A4	~$
¥	A5	~%
¦	A6	~&
§	A7	~'
¨	A8	~(
©	A9	~)
ª	AA	~*
«	AB	~+
¬	AC	~,
(soft hyphen)	AD	~- (Dash)
×	D7	~W
Ø	D8	~X
Ù	D9	~Y
Ú	DA	~Z

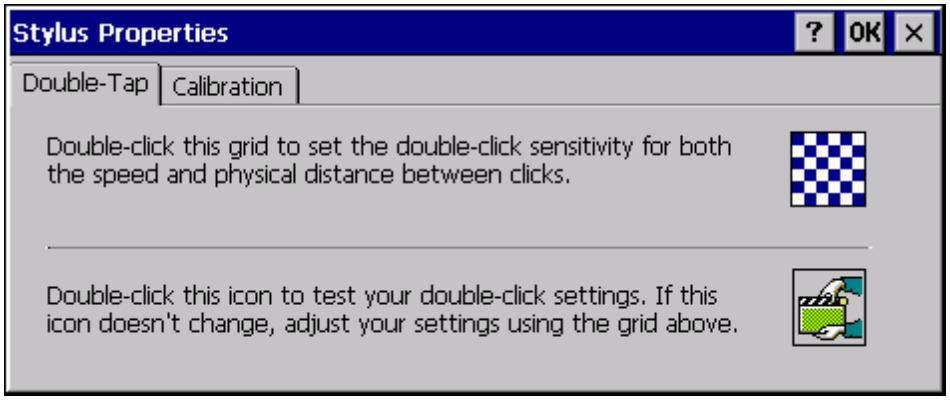
Desired ASCII	Hex Value	Hat Encoded
²	B2	~2
³	B3	~3
´	B4	~4
µ	B5	~5
¶	B6	~6
·	B7	~7
¸	B8	~8
¹	B9	~9
º	BA	~:
»	BB	~;
¼	BC	~<
½	BD	~=
¾	BE	~>
¿	BF	~?
À	C0	~@
Á	C1	~A
Â	C2	~B
Ã	C3	~C
Ä	C4	~D
Å	C5	~E
Æ	C6	~F
Ç	C7	~G
È	C8	~H
É	C9	~I
Ê	CA	~J
Ë	CB	~K
Ì	CC	~L
Í	CD	~M
Î	CE	~N
Ï	CF	~O
Ð	D0	~P
Ñ	D1	~Q
Ò	D2	~R
Ó	D3	~S
Ô	D4	~T
Õ	D5	~U
Ö	D6	~V

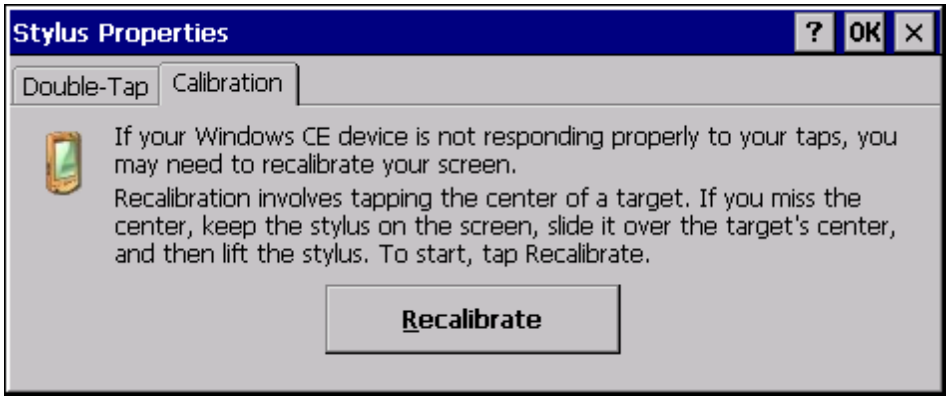
Desired ASCII	Hex Value	Hat Encoded
Û	DB	~[
Ü	DC	~\\
Ý	DD	~]
Þ	DE	~\^
ß	DF	~_ (Underscore)
à	E0	~`
á	E1	~a
â	E2	~b
ã	E3	~c
ä	E4	~d
å	E5	~e
æ	E6	~f
ç	E7	~g
è	E8	~h
é	E9	~i
ê	EA	~j
ë	EB	~k
ì	EC	~l
í	ED	~m
î	EE	~n
ï	EF	~o
ð	F0	~p
ñ	F1	~q
ò	F2	~r
ó	F3	~s
ô	F4	~t
õ	F5	~u
ö	F6	~v
÷	F7	~w
ø	F8	~x
ù	F9	~y
ú	FA	~z
û	FB	~{
ü	FC	~|
ý	FD	~}
þ	FE	~~
ÿ	FF	~^?

Stylus

Start > Settings > Control Panel > Stylus

Use this control panel option to set stylus double-tap sensitivity properties and calibrate the VX7 touch panel when needed.


Stylus Properties
?
OK
Double-Tap
Calibration
Double-click this grid to set the double-click sensitivity for both the speed and physical distance between clicks.
Double-click this icon to test your double-click settings. If this icon doesn't change, adjust your settings using the grid above.


Stylus Properties
?
OK
Double-Tap
Calibration
If your Windows CE device is not responding properly to your taps, you may need to recalibrate your screen.
Recalibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus. To start, tap Recalibrate.
Recalibrate

Double Tap

Follow the instructions on the screen and tap the OK button to save any double tap changes.

Calibration Tab

Calibration involves tapping the center of a target. If you miss the center, keep the stylus on the screen, slide it over the target's center, and then lift the stylus.

To begin, tap the **Recalibrate** button on the screen with the stylus. Press and hold the stylus on the center of the target as it moves around the screen. Press the Enter key to keep the new calibration setting or press the Esc key to revert to the previous calibration settings.

System

Start > Settings > Control Panel > System

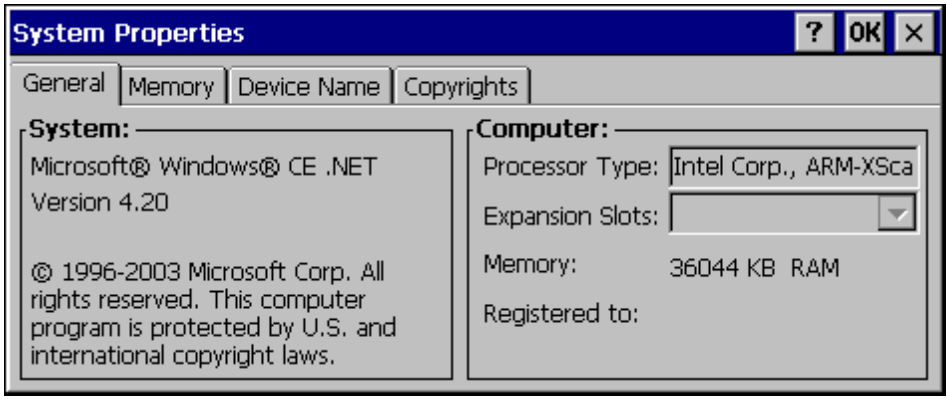
Use these VX7 panels to:

- Review System and mobile device data and revision levels.
- Adjust Storage and Program memory settings.
- Assign a device name and device descriptor.

Factory Default Settings

General	No user interaction
Memory	1/3 storage, 2/3 program memory
Device Name	Unique to equipment type
Device Description	LXE_VX7 or LXE_VX7SD *unique to equipment type*
Copyrights	No user interaction

General Tab

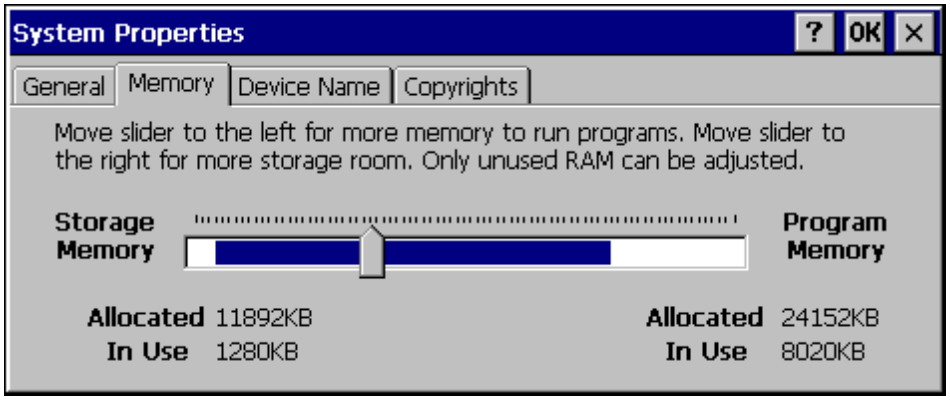


System: This screen is presented for information only. The System parameters cannot be changed by the user.

Computer: The processor type is listed. The type cannot be changed by the user. Total computer memory and the identification of the registered user is listed and cannot be changed by the user.

Memory sizes given do not include memory used up by the operating system. For example, a system with 128 MB may only report 99 MB memory, since 29 MB is used by the operating system. This is actual DRAM memory, and does not include internal flash used for storage.

Memory Tab

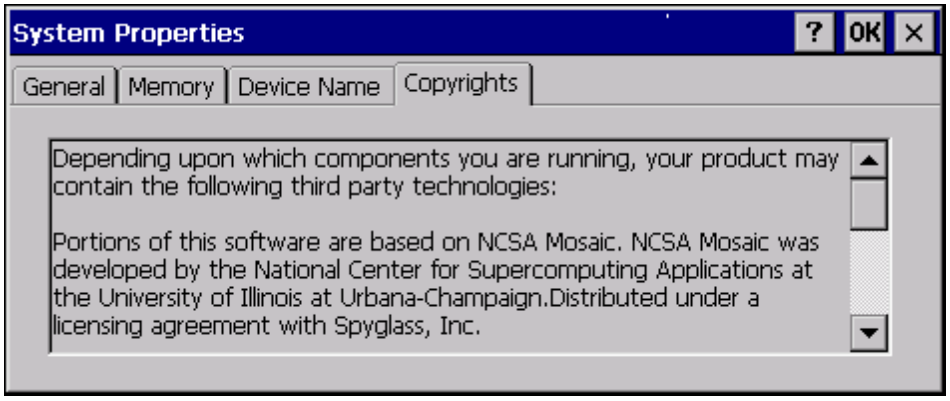


Move the slider to allocate more memory for programs or storage. If there isn't enough space for a file, increase the amount of storage memory. If the mobile device is running slowly, try increasing the amount of program memory.

Device Name Tab

The device name and description can be changed by the user. Enter the name and description using either the keypad or the Input Panel and tap OK to save the changes. This information is used to identify the VX7 to other computers and devices.

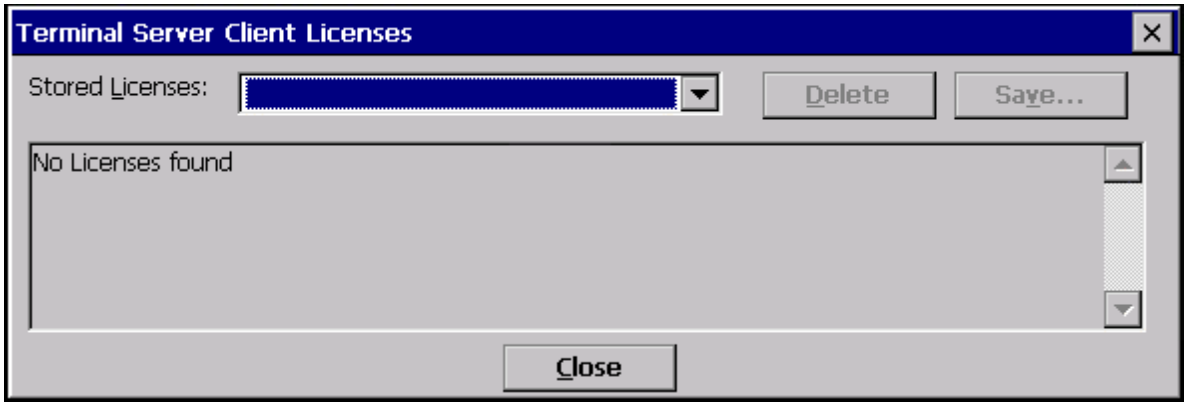
Copyrights Tab


System Properties
?
OK
General
Memory
Device Name
Copyrights
Depending upon which components you are running, your product may contain the following third party technologies:
Portions of this software are based on NCSA Mosaic. NCSA Mosaic was developed by the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.Distributed under a licensing agreement with Spyglass, Inc.

This screen is presented for information only. The Copyrights information cannot be changed by the user.

Terminal Server Client Licenses

Start > Settings > Control Panel > Terminal Server Client Licenses



Any licenses stored on the VX7 appear in the drop-down list. Select a license and tap the Close button. The license is available for use immediately.

Volume and Sounds

Start > Settings > Control Panel > Volume & Sounds

Note: An application may override the control of the speaker volume. Turning off sounds saves power and prolongs battery life.

Set volume parameters and assign sound WAV files to CE events using these options.

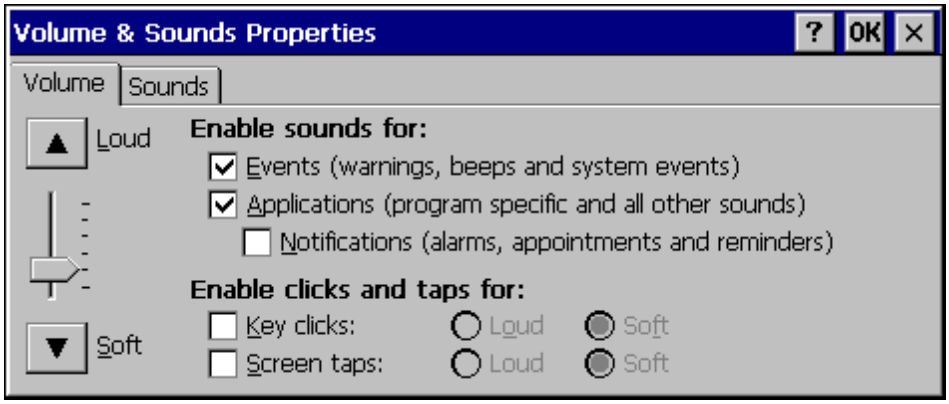
You can also select / deselect sounds for key clicks and screen taps and whether each is loud or soft.

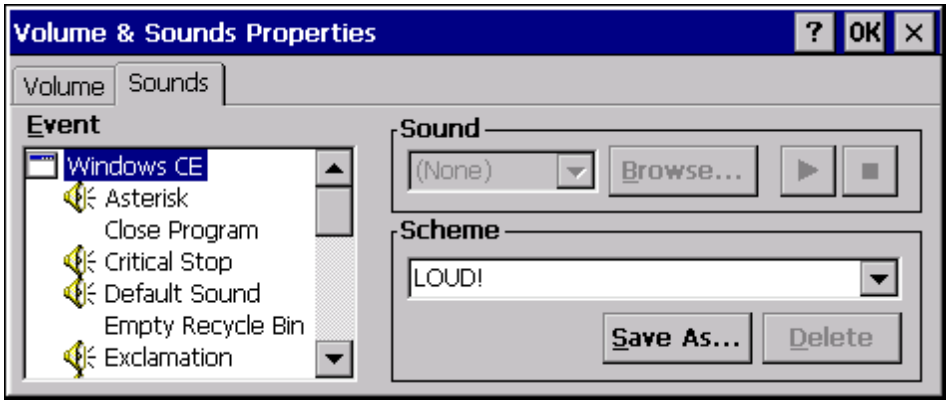
As the volume scrollbar is moved between Loud and Soft, the VX7 emits a tone each time the volume increases or decreases.

Volume must be enabled when you want to adjust volume settings using keypad keys.

Factory Default Settings

Volume	
Events	Enabled
Application	Enabled
Notifications	Disabled
Volume	Middle of Bar
Key click	Disabled
Screen tap	Disabled
Sounds	
Scheme	LOUD!





The volume setting is stored in the registry and is recalled at power on.

Note: Rejected barcodes generate a bad scan beep. In some cases, the receipt of data from the scanner triggers a good scan beep from a tethered scanner, and then the rejection of scanned barcode data by the barcode processing causes a bad scan beep from the mobile device on the same data.

Good Scan and Bad Scan Sounds

Good scan and bad scan sounds are stored in the Windows directory, as SCANGOOD.WAV and SCANBAD.WAV. These are unprotected WAV files and can be replaced by a WAV file of the user's choice.

By default a good scan sound on the VX7 is a single beep, and a bad scan sound is a double beep.

WiFi

Start > Settings > Control Panel > WiFi or click the Summit Client Utility icon

Use this option to set parameters and manage profiles for the wireless client pre-loaded on your VX7. See the Summit Client Utility for more information.

Chapter 4: Enabler Installation and Configuration

Introduction

This section discusses Honeywell supported features with Wavelink Avalanche Mobile Device Servers. This section is split into three basic areas:

- Installation
- User Interface
- Enabler Configuration

Installation

To use the Wavelink Avalanche MC System, the following items are required:

- A desktop or laptop PC on which to install the Avalanche MC Console.
- A desktop or laptop PC on which to install the Avalanche Mobile Device Server (this can be the same PC where the Avalanche MC Console is installed).
- Wavelink Avalanche MC Console 4.2 or later.
- A Wavelink Device License for each client device.

To use Avalanche Remote Control, the follow additional items are required:

- Wavelink Remote Control plug-in, 2.0 or later
- A Wavelink Remote Control License for each client device

Installing the Enabler on Mobile Devices

Supported devices have the Avalanche Enabler installation files loaded, but not installed, on the mobile device when it is shipped. The installation files are located in the \System folder on Windows devices.

Supported devices manufactured before April 2007 must have some software components upgraded before they can use the Avalanche Enabler functions described in this reference guide. Contact Technical Assistance for details on upgrading the mobile device baseline.

Note: If the user is NOT using Wavelink Avalanche to manage their mobile device(s), the Enabler should not be installed on the mobile device(s). Doing so results in unnecessary delays when booting the device.

The Avalanche Enabler installation file LXE_ENABLER.CAB is loaded on the VX7 by Honeywell; however, the device is not configured to launch the Enabler installation file automatically. The installation application must be run manually the first time Avalanche is used.

Note: Older versions of the Enabler may have a device specific name such as LXE_XXX_ENABLER.CAB.

After installation, the Enabler runs as a background application monitoring for updates. This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler interface.

This behavior can be modified by accessing the Avalanche Update Settings panel through the Enabler Interface.

The RMU.CE.CAB file is placed on the device during manufacturing in the \System\RMU folder.

During the Enabler installation process, the Enabler checks for the RMU.CE.CAB file in the \System folder.

- If present, it assumes the RMU.CE.CAB file is already installed and continues.
- If the file RMU.CE.CAB file is not present, it looks for the file in the \System\RMU folder.
- If present, the Enabler copies the file to the \System folder and installs it.

At this point, the OS will automatically install the Remote Management Utility (RMU) after the VX7 reboots.

VX6/VX7 Enabler Installation

Because the VX6 and VX7 computers have two possible network adapters (the optional internal adapter for a cabled network connection and the wireless network card), the Enabler uses the first network adapter it discovers. In order to assure the Enabler uses the wireless connection, perform one of the following actions:

- Select the Adapters tab in the Enabler setup (See Enabler Configuration) and make sure the wireless adapter is selected for **Current Adapter**.
- To **disable** the internal network adapter, create a file in the \System directory named **NoEther.tag**. The contents of the file are unimportant; but the file must be named NoEther.tag and it must be in the \System directory. (If the \System directory contains a file named **Ether.tag**, you can rename this file to NoEther.tag instead of creating a new file).
- After creating the file, coldboot the device. After the device finishes booting, the internal Ethernet adapter is disabled.
- To **restore** the adapter, delete the NoEther.tag file and coldboot the device.

Enabler Uninstall Process

To remove the Avalanche Enabler from the VX7:

- Delete the Avalanche folder located in the \System directory.
- Warm boot the VX7.

The Avalanche folder cannot be deleted while the Enabler is running. See Stop the Enabler Service.

If sharing errors occur while attempting to delete the Avalanche folder, warm boot the VX7, immediately delete the Avalanche folder, and then perform another warm boot.

Stop the Enabler Service

To stop the Enabler from monitoring for updates from the Mobility Center Console:

1. Open the Enabler Settings Panels by tapping the Enabler icon on the VX7 desktop.
2. Select **File > Settings**.
3. Select the **Startup/Shutdown** tab.
4. Select the **Do not monitor or launch Enabler** parameter to prevent automatic monitoring upon startup.
5. Select **Stop Monitoring** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.
6. Click the **OK** button to save the changes.
7. **Reboot** the VX7 if necessary.

or

1. Open the Enabler Settings Panels by tapping the Enabler icon on the VX7 desktop.
2. Select **File > Settings**.
3. Select the **Preferences** tab.
4. Select **Do not monitor** to prevent automatic monitoring upon **Startup**.
5. Select **Exit Application** for an immediate shutdown of all Enabler update functionality upon exiting the user interface.

6. Click the **OK** button to save the changes.
7. **Reboot** the VX7 if necessary.

Update Monitoring Overview

There are three methods by which the Enabler on the VX7 can communicate with the Mobile Device Server running on the host machine.

- Wired via a serial cable between the Mobile Device Server PC and the VX7.
- Wired via a USB connection, using ActiveSync, between the Mobile Device Server PC and the VX7.
- Wirelessly via the VX7 2.4GHz radio and an access point

After installing the Enabler on the VX7 the Enabler searches for a Mobile Device Server, first by polling all available serial ports and then over the wireless network.

The Enabler running on the VX7 will attempt to access COM1, COM2, and COM3. “Agent not found” will be reported if the Mobile Device Server is not located or a serial port is not present or available (COM port settings can be verified using the bar code wedge panels on the VX7).

The wireless connection is made using the default wireless [radio] interface on the mobile device therefore the VX7 must be actively communicating with the network for this method to succeed.

If a Mobile Device Server is found, the Enabler automatically attempts to apply all wireless and network settings from the active profile. The Enabler also automatically downloads and processes all available packages.

If the Enabler does not automatically detect the Mobile Device Server, the IP address of the Mobile Device Server can be entered on the Connect tab of the Enabler setup. Please see Enabler Configuration for details.

Mobile Device Wireless and Network Settings

Once the connection to the Mobile Device Server is established, the VX7 Enabler attempts to apply all network and wireless settings contained in the active profile.

The success of the application of settings is dependent upon the local configuration of control parameters for the Enabler.

These local parameters cannot be overridden from the Avalanche MC Console.

The default Enabler adapter control settings are:

- Manage network settings – enabled
- Use Avalanche network profile – enabled
- Manage wireless settings – disabled

To configure the Avalanche Enabler management of the network and wireless settings:

1. Open the Enabler Settings Panels by tapping the **Enabler icon** on the desktop.
2. Select **File > Settings**.
3. Select the **Adapters** tab.
4. Choose settings for the **Use Manual Settings** parameter.
5. Choose settings for **Manage Network Settings**, **Manage Wireless Settings** and **Use Avalanche Network Profile**.
6. Click the **OK button** to save the changes.
7. **Reboot** the device.

Preparing a Device for Remote Management

Two additional utilities are necessary for remote management. These utilities are included on mobile devices manufactured after April 2007.

- The **Remote Management Utility (RMU)** must be installed on all mobile devices first – then you can control mobile device reboot, storage RAM adjustment, real-time updates and Avalanche Enabler properties. If the RMU is not already installed on the VX7, see Using Wavelink Avalanche to Upgrade System Baseline.
  If in doubt, verify RMU.CE.CAB exists in the \System folder. If the RMU.CE.CAB file is present when the Enabler is installed, the RMU is also installed.

  If the OS package includes double-byte Asian fonts, the storage RAM property of the RMU must be higher than the default value (40MB).

  If the amount of storage RAM is too low, the Enabler returns a “Mobile unit out of resources” error.

  To determine the minimum value required, inspect the RMU.StorageRAM>=*nn* parameter in the Criteria field for the OS package. Generally, this setting should be approximately 40 MB above the amount of RAM in use on the device for a standard OS and 50MB above the amount of RAM in use for an OS with Asian fonts.

  For example, if after installing all the software, the device shows 5MB in use, this setting should be about 45MB for a standard OS, 55 MB for an Asian font OS.
- Use the **Wireless Configuration Application (WCA)** when you want to remotely manage the Summit client device. This utility is downloaded and installed in addition to the Remote Management Utility. The WCA is included when the Summit radio driver software is updated. The WCA is automatically installed when the radio driver is updated.

If the Remote Management Utility (RMU) is not present on the VX7, see Using Wavelink Avalanche to Upgrade System Baseline.

Using Wavelink Avalanche to Upgrade System Baseline

This procedure assumes the Avalanche Enabler is already installed on the VX7 and is already in communication with the Avalanche MC Console.

Part 1 – Bootstrapping the RMU

1. Install the RMUCEbt package into the Avalanche MC Console. Do NOT include the Reboot option as part of the configuration (i.e. the **Reboot button** in the "Reboot Options" branch must be unbolded).
2. Enable ONLY the RMUCEbt package in the Avalanche MC Console and update the devices. The RMU is downloaded and automatically installed.
3. **Disable** the RMUCEbt package in the Avalanche MC Console.
4. For each device, **double-click** on the device to open the Client Controls dialog box.
5. Check the **Delete Orphaned Packages** checkbox and click the **Update Now** button.
6. After the sync completes, uncheck **Delete Orphaned Packages** and close the dialog box.

Part 2 – Installing Packages

1. **Enable** the RMUCE package in the Avalanche MC Console.
2. **Enable** all remaining packages and send them down. It is important that you include the new OS package in this group (be sure to include the Enabler). If the radio is to be managed remotely, it is important to include the radio package in this group so that after the reboot the radio can automatically associate. If the radio package is not sent, the device loses connection to the network and manual configuration of the radio parameters is required.
3. Set the Reboot setting for the OS package to **Auto**.
4. After all packages are downloaded (this may take several minutes) the Remote Management Utility (RMU) is launched. The RMU processes all the downloaded packages. If the radio package was downloaded, the Wireless Configuration Application (WCA) is launched to process the new radio settings.
5. After the RMU finishes installing all the packages, the device is automatically coldbooted (assuming the Reboot setting was set to Auto in Step 3).
6. After the Device completes the coldboot, the RMU is autoinstalled by the OS and the previously downloaded packages are restored. Assuming at least one package has registry settings that were restored, and that package was set to reboot (either auto or prompt), the RMU then performs an automatic warmboot.
7. After the warmboot, the device is configured.
8. If the device will no longer be monitored by Wavelink Avalanche, you may remove the Enabler to eliminate boot up delays, if desired. Even if the Enabler is removed, the installed packages and their configurations continue to be restored with every reboot by the RMU.

Version Information on Mobile Devices

The VersionInfo.EXE file is included in the Remote Management Utility package downloaded to the VX7. It is stored in the \Program Files\RMU folder. When VersionInfo.EXE is opened, a dialog box is presented to the VX7 user displaying:

- Remote Management Utility (RMU) version
- Wireless Configuration Application (WCA) version

VersionInfo displays the version for each utility only after that utility has been executed at least once.

User Interface

The Enabler can be configured and controlled manually through the user interface on the VX7. This section details the functionality that can be controlled by the user or system administrator.

Parameters and Screen Displays

Screen displays shown in this section are designed to present the end-user with information graphically.

Placement of information on the screen displays may be split between one or many tabbed panels.

Standard Avalanche Enabler parameters that are not supported by Honeywell may be missing or dimmed (visible but unable to be edited) on the tabbed panels or screen displays.

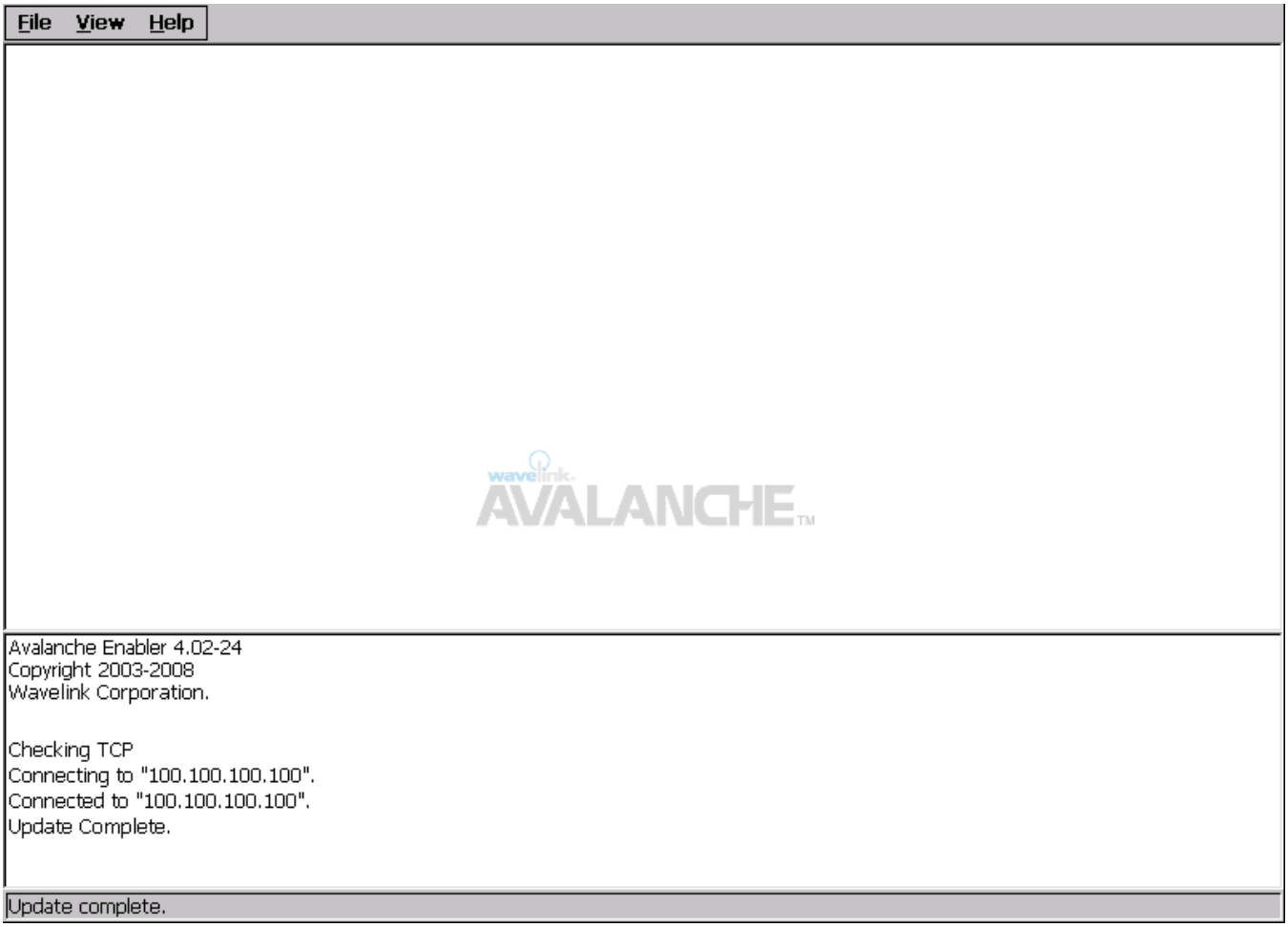
Enabler Configuration

Depending on the version of the Enabler running on the VX7, the desktop Enabler icon may look like one of the following:

The available configuration options and tabs may vary by Enabler version. The examples shown in this section assume the latest version of the Enabler is installed on the VX7.

The Enabler user interface application is launched by clicking either the **Enabler icon** on the desktop or Taskbar or by selecting **Avalanche Enabler** from the Programs menu.

The opening screen presents the VX7 user with the connection status and a navigation menu.



Note: Some parameters and features described in this section may not be available if you are not running the latest version of the Enabler. Contact Technical Assistance for upgrades.

File Menu Options

Connect	The Connect option under the File menu allows the user to initiate a manual connection to the Mobile Device Server. The connection methods, by default, are wireless and COM connections. Any updates available will be applied to the VX7 immediately upon a successful connection.
Scan Config	*The Scan Configuration feature is not supported.* The Scan Config option under the File menu allows the user to configure Enabler settings using a special bar code that can be created using the Avalanche MC Console utilities. Refer to the Wavelink Avalanche Mobility Center User Guide for details.
Settings	The Settings option under the File menu allows the VX7 user to access the control panel to locally configure the Enabler settings. The Enabler control panel is, by default, password protected. The default Settings password is **system**. The password is not case-sensitive.

Avalanche Update using File > Settings

Use these menu options to setup the Avalanche Enabler on the VX7. Change the settings and save them by rebooting before connecting to the network.

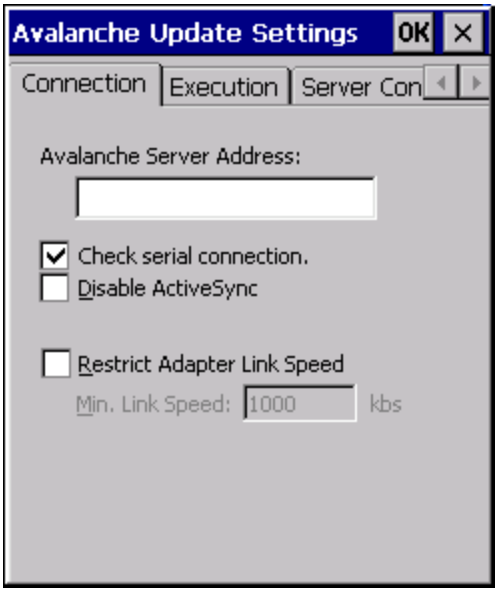
Alternatively, the Mobile Device Server can be disabled until needed (refer to the **Wavelink Avalanche Mobility Center User's Guide** for details).

Menu Options

Note: Your VX7 screen display may not be exactly as shown in the following menu options. Contact Technical Assistance for version information and upgrade availability.

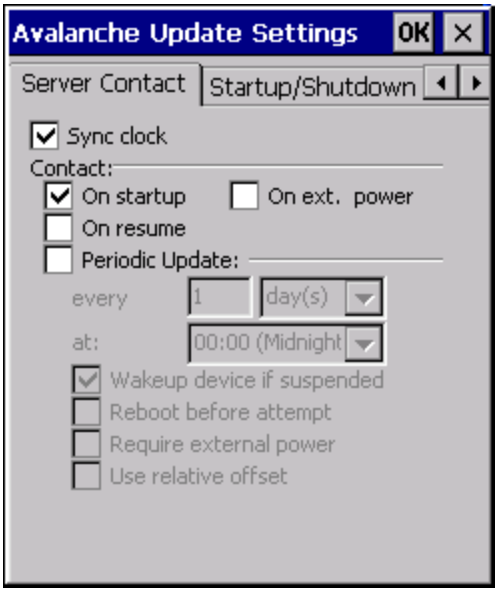
Connection	Enter the IP Address or host name of the Mobile Device Server. Set the order in which serial ports or RF connections are used to check for the presence of the Mobile Device Server.
Server Contact	Setup synchronization, scheduled Mobile Device Server contact, suspend and reboot settings.
Data	Control when data is transferred between the device and the Mobile Device Server.
Preferences	Set options for Enabler startup or shutdown and logging. If the Preferences tab is not present, you may have an older version of the Enabler with the Startup/Shutdown tab.
Display	Set up the Windows display at startup, on connect and during normal mode. The settings can be adjusted by the user.
Taskbar	Set options for Taskbar. If the Taskbar tab is not present, you may have an older version of the Enabler with the Startup/Shutdown tab.
Execution	*Not available in this release*. Use AppLock instead, which is resident on each device.
Scan Config	This option allows the user to configure Enabler settings using a special bar code that is created by the Avalanche MC Console. *Scan Config not currently supported.*
Shortcuts	Add, delete and update shortcuts to user-allowable applications.
SaaS	Configure the Enabler to connect with Avalanche on Demand.
Adapters	Enable or disable network and wireless settings. Select an adapter and switch between the Avalanche Network Profile and manual settings.
Status	View the current adapter signal strength and quality, IP address, MAC address, SSID, BSSID and Link speed. The user cannot edit this information.
Startup/Shutdown	Set options for Enabler program startup or shutdown. Replaced by Preferences and Taskbar tabs in some versions of Enabler.

Connection



Avalanche Server Address	Enter the IP Address or host name of the Mobile Device Server assigned to the VX7.
Check Serial Connection	Indicates whether the Enabler should first check for serial port connection to the Mobile Device Server before checking for a wireless connection to the Mobile Device Server.
Disable Active-Sync	Disable ActiveSync connection with the Mobile Device Server.
Restrict Adapter Link Speed	Default is disabled. Minimum Link Speed dimmed. When enabled, the Enabler only allows a connection to the server if the detected link speed is greater than or equal to the specified value.

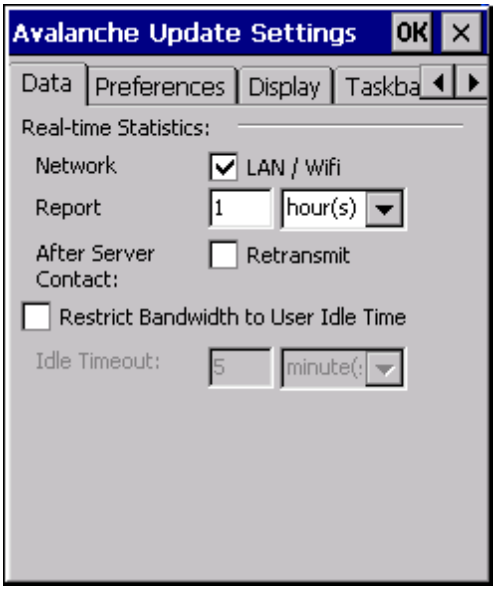
Server Contact



Note: Your VX7 screen display may not be exactly as shown above. Contact Technical Assistance for upgrade availability and version information.

Sync Clock	Reset the time on the VX7 based on the time on the Mobile Device Server host PC.
Contact	On Startup – Connect to the Mobile Device Server when the Enabler is accessed.
	On Resume – Connect to the Mobile Device Server when resuming from Suspend mode.
	On IP Change – Connect to the Mobile Device Server when the IP address of the VX7 changes.
	On Ext. Power – Initiate connection to the Mobile Device Server when the device is connected to an external power source, such as based on a docking event.
Contact Periodically / Periodic Update	Allows the administrator to configure the Enabler to contact the Mobile Device Server and query for updates at a regular interval beginning at a specific time.
Wakeup device if suspended	If the time interval for periodic contact with the Mobile Device Server occurs, a mobile device that is in Suspend Mode can wakeup and process updates.
Reboot before attempt	Reboot mobile device before attempting to contact Mobile Device Server.
Require external power	Only connect when the mobile device has external power.
Use relative offset	Dimmed.

Data



The Data tab controls when data is transferred between the VX7 and the Mobile Device Server.

Network	When checked, the LAN/WiFi network is enabled to transfer statistics.
Report	Specifies the Report Interval, how frequently the Enabler reports statistics to the Mobile Device Server.
Retransmit After Server Contact	Specifies if the device sends statistics to the Mobile Device Server immediately following a connection to the server.
Restrict Bandwidth to User Idle Time	When enabled, periodic updates from the Mobile Device Server are postponed until the VX7 has been idle for the specified period of time. The default is disabled.
Idle timeout	Specify the length of time the device must be idle before a periodic update can run, used when the parameter above is enabled.

Preferences

For best results, use *AppLock* to manage the taskbar. AppLock is resident on each mobile device.

If the Preferences tab is not present on the Enabler installed on your device, please see the equivalent options on the Startup/Shutdown tab.

Administration

By default, *Keep settings unlocked for 10 minutes* is disabled (checkbox is blank).

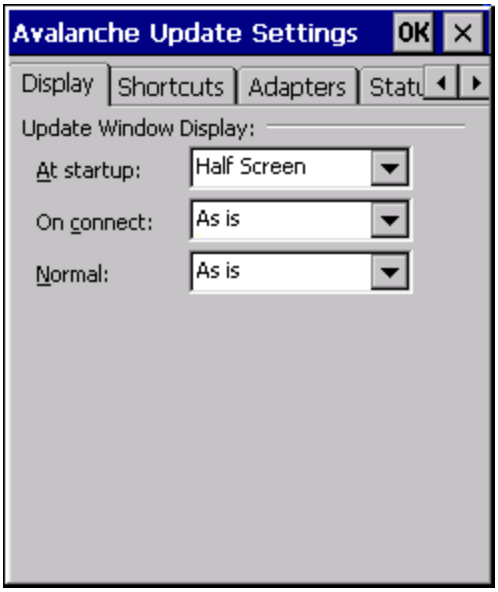
Application

Startup	Behavior of the Enabler when the VX7 boots up. The default is Monitor for Updates. • Do not Monitor - When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server. • Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application. • Launch User Interface - Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Shutdown	Behavior of the monitor when the Enabler is exited. The default is Monitor for Updates. • Monitor for Updates - Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application. • Exit Application - Terminates the monitor (requires successful password entry if a password has been configured).

Activity Log

Log Level	Use this option to control the level of detail recorded in the log file. The default is No Activity Log. • No Activity Log - No log file is written. • Critical - Only critical errors written to the log files. • Error - Communication or configuration problems are written to the log file along with critical messages. • Warning - Possible operation problems are written to the log file along with critical and error messages. • Info - Operational information is written to the log file. • Debug - The most detailed log file.
Display Level	Use this option to control the level of detail shown on the main Enabler screen. The default is Basic Output. • Basic Output - General information is displayed. • Critical - Critical errors are displayed in addition to those above. • Error - Communication or configuration problems are displayed in addition to those above. • Warning - Possible operation problems are displayed in addition to those above. • Info - Operational information is displayed in addition to those above. • Debug - The most detailed list is displayed. .

Display



Update Window Display

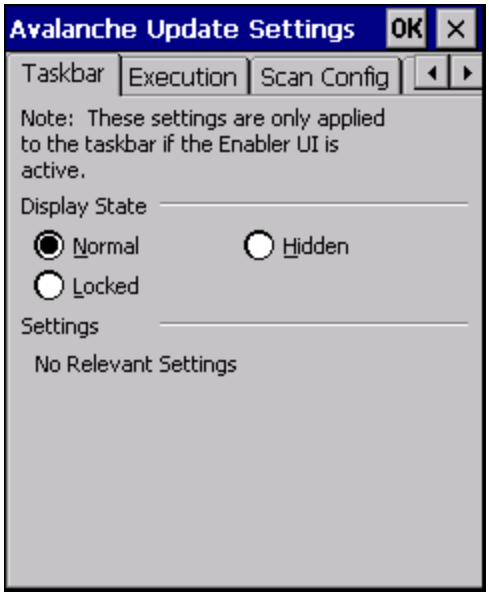
The user interface for the Enabler can be configured to dynamically change based on the status of the VX7 connection with the Mobile Device Server.

At startup	Default is Half Screen. Options are Half screen, Hidden or Full screen.
On connect	Default is As Is. Options are As is, Half screen, or Full screen.
Normal	Default is As Is. Options are Half screen, Hidden or As Is.

Taskbar

For best results, use *AppLock* to manage the taskbar. AppLock is resident on each mobile device.

If the Taskbar tab is not present on the Enabler installed on your device, please see the equivalent options on the Startup/Shutdown tab.



The Display State options control the appearance of the taskbar while using the Enabler interface.

- Normal - taskbar is visible, taskbar icons function normally.
- Hidden - taskbar is not displayed
- Locked - taskbar is visible, but most icons are hidden or for information only.

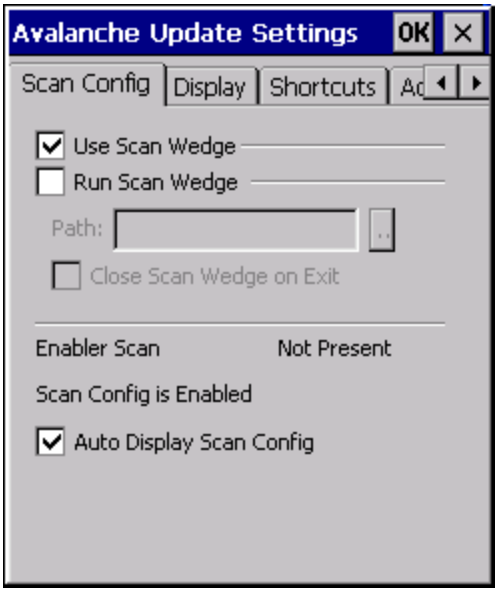
Execution

Note the dimmed options on this VX7 panel. This menu option is designed to manage downloaded applications for automatic execution upon startup.

Auto-Execute Selection	An application that has been installed with the Avalanche Management system can be run automatically following each boot.
Select Auto-Execute App	The drop-down box provides a list of applications that have been installed with the Avalanche Management System.
Delay before execution	Time delay before launching Auto-Execute application.

Scan Config

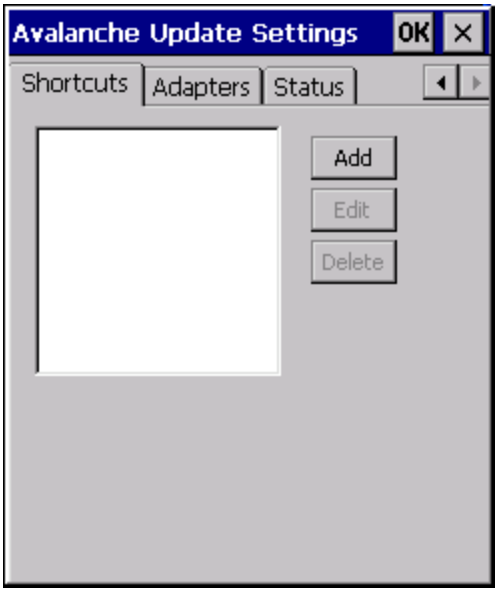
For best results, use *eXpress Config* and *eXpress Scan* for this function. eXpress Scan is included with the updated VX7 enablers.



Scan Config functionality is a standard option of the Wavelink Avalanche MC system but is *not currently supported* on the VX7.

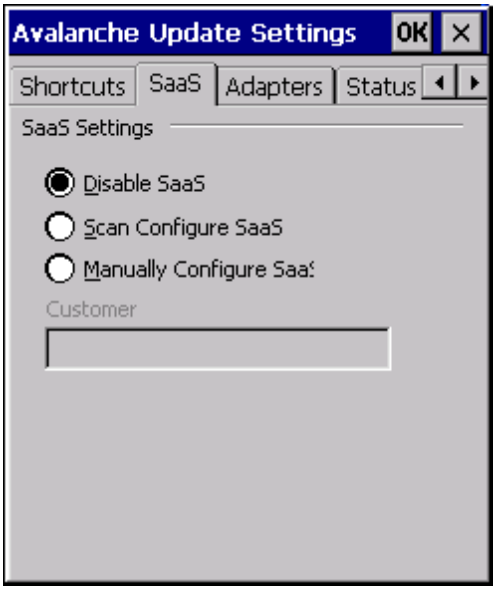
Shortcuts

For best results, use *AppLock* for this function. AppLock is resident on each mobile device.



Configure shortcuts to other applications on the VX7. Shortcuts are viewed and activated in the Programs panel. This limits the user's access to certain applications when the Enabler is controlling the mobile device display.

SaaS

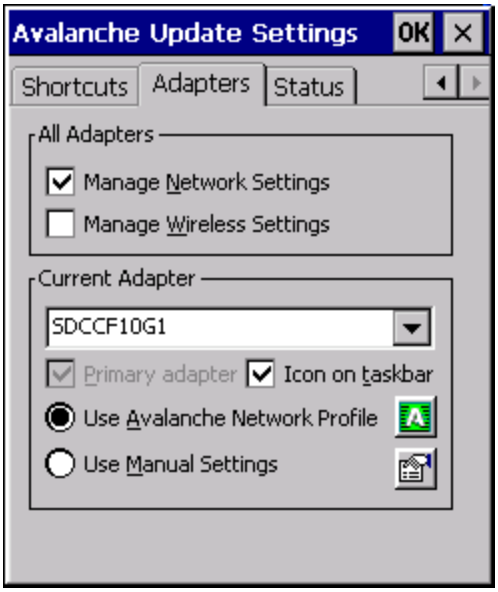


Use to configure the Enabler to connect with Avalanche on Demand. This is a Software-as-a-Service version of Avalanche. Using either of the SaaS configuration options below assumes the user has registered with Wavelink.

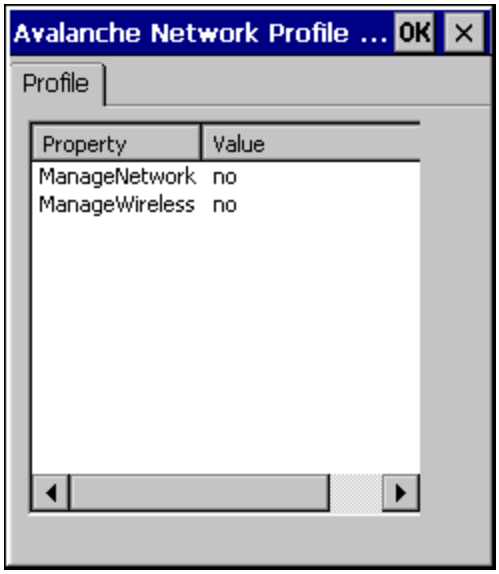
Disable SaaS	No SaaS connection is used.
Scan Configure SaaS	Scan bar codes printed from within the Avalanche Console to configure the Enabler for the SaaS connection.
Manually Configure SaaS	Manually enter the SaaS connection information. Enter the server address on the Connection tab and the customer ID in the Company textbox.

Adapters

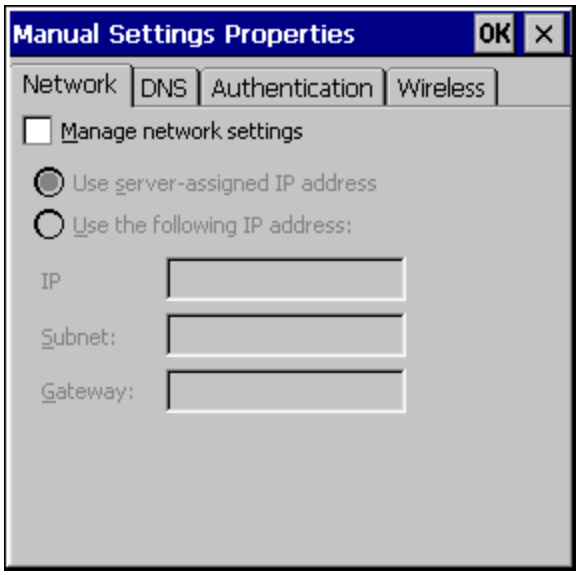
Note: Review the network settings configuration utilities and the default values before setting All Adapters to Enable in the Adapters applet.



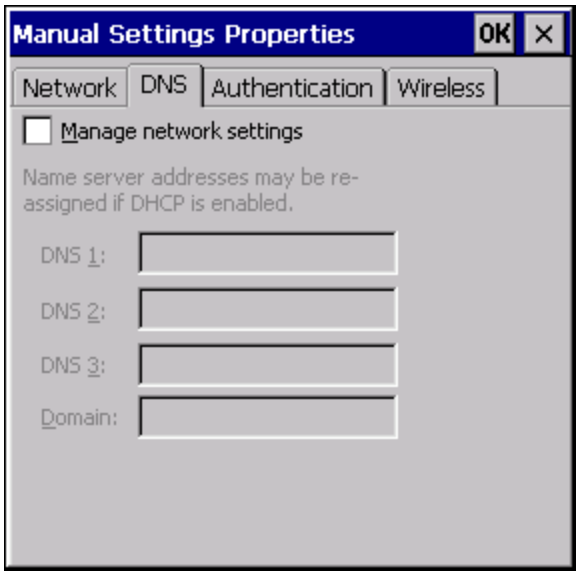
Manage Network Settings	When enabled, the Enabler will control the network settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is enabled by default.
Manage Wireless Settings	When enabled, the Enabler will control the wireless settings. This parameter cannot be configured from the Avalanche Mobility Center Console and is disabled by default. For Summit clients, Manage Wireless Settings should not be checked as configuration packages provide more radio configuration options.
Current Adapter	Lists all network adapters currently installed on the VX7.See special instructions for VX7.
Primary Adapter	Indicates if the Enabler is to attempt to configure the primary adapter (active only if there are multiple network adapters).
Icon on taskbar	Places the Avalanche icon in the Avalanche taskbar that may, optionally, override the standard Windows taskbar.
Use Avalanche Network Profile	The Enabler will apply all network settings sent to it by the Mobile Device Server.
Avalanche	Selecting the Avalanche Icon will access the Avalanche Network Profile tab which will display current network settings.

Icon (varies by Enabler version) 	
Use Manual Settings	When enabled, the Enabler will ignore any network or wireless settings coming from the Avalanche MC Console and use only the network settings on the VX7.
Properties Icon	Selecting the Properties icon displays the Manual Settings Properties dialog applet. From here, the user can configure Network, DNS and Wireless parameters using the displays shown below:

Note: A reboot may be required after enabling or disabling these options.

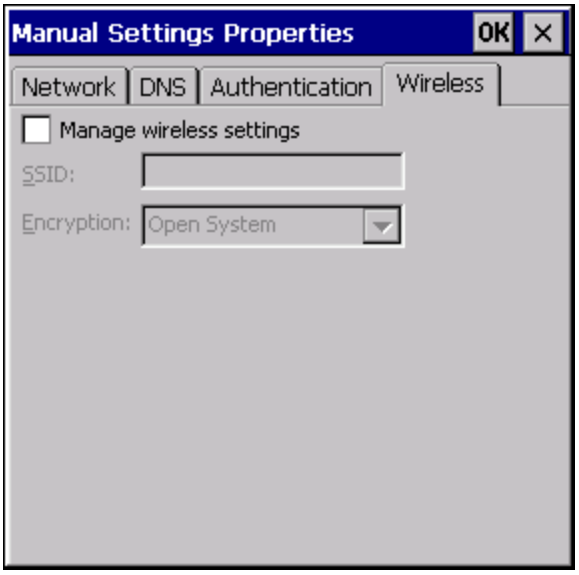


Network



DNS

Authentication



Wireless

Note: The Authentication tab may not be present in all versions of the Enabler.

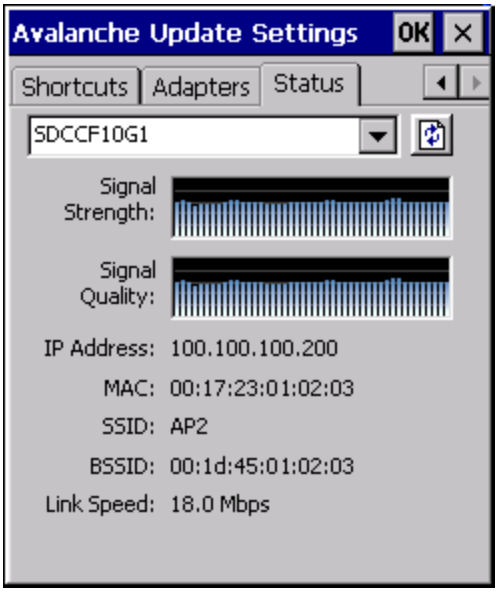
It is not recommend to enable “Manage Wireless Settings” for Summit Client devices.

When you download a profile that is configured to manage network and wireless settings, the Enabler will not apply the manage network and wireless settings to the adapter unless the global Manage wireless settings and Manage network settings options are enabled on the Adapters panel (see Figure titled Adapters Options – Network, earlier in this section). Until these options are enabled, the network and wireless settings are controlled by the third-party software associated with these settings.

Status

The Status panel displays the current status of the VX7 network adapter selected in the drop down box. Note the availability of the Windows standard Refresh button.

When the Windows Refresh button is tapped, the signal strength, signal quality and link speed are refreshed for the currently selected adapter. It also searches for new adapters and may cause a slight delay to refresh the contents of the drop-down menu.

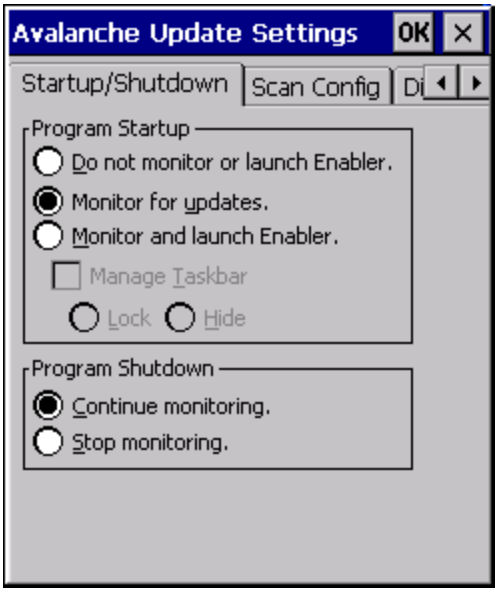


Link speed indicates the speed at which the signal is being sent from the adapter to the VX7. Speed is dependent on signal strength.

Startup/Shutdown

For best results, use *AppLock* to manage the taskbar. AppLock is resident on each mobile device.

If the Startup/Shutdown tab is not present on the Enabler installed on your device, please see the equivalent options on the Preferences tab and the Taskbar tab.



Do not monitor or launch Enabler	When the device boots, do not launch the Enabler application and do not attempt to connect to the Mobile Device Server.
Monitor for updates	Attempt to connect to the Mobile Device Server and process any updates that are available. Do not launch the Enabler application.
Monitor and launch Enabler	Attempt to connect to the Mobile Device Server and process any updates that are available. Launch the Enabler application.
Manage Taskbar (Lock or Hide)	Note the dimmed options. The Enabler can restrict user access to other applications when the user interface is accessed by either locking or hiding the taskbar.
Program Shutdown (Continue or Stop monitoring)	The system administrator can control whether the Enabler continues to monitor the Mobile Device Server for updates once the Enabler application is exited.

Exit

The Exit option is password protected. The default password is **leave**. The password is not case-sensitive.

Depending on the behavior chosen for the Shutdown parameter, the following screen may be displayed:

Note: The icon on the screen above may differ based on the version of the Enabler installed on the VX7.

Change the option if desired. Tap the X button to cancel Exit. Tap the OK button to exit the Avalanche applet.

Using Remote Management

1. Configure the radio to connect to the network running the Mobile Device Server. After the VX7 is connected, proceed to step 2.
2. If it is desired to configure the radio using the Summit package, add the configured package to the Wavelink Avalanche MC Console and enable it.
3. Verify RMU.CE.CAB exists in the \System\RMU folder.
4. Double click the VX7 enabler CAB file in the \System folder.
5. The enabler automatically launches after installation and contacts the Mobile Device Server. The Avalanche MC Console connected to that Mobile Device Server identifies the remote device and performs a sync. This downloads any available packages available for the VX7.

Using eXpress Scan

eXpress Scan Desktop Icon

If the VX7 has an eXpress Scan icon on the desktop, eXpress Scan may be used for the initial configuration of the device.

If the eXpress Scan icon is not present on the desktop, install the Enabler. If the icon is still not present, the Enabler must be updated.

If the eXpress Scan icon is present, follow these steps to configure the VX7 to connect with the wireless network and the Mobile Device Server.

Step 1: Create Bar Codes

Bar codes are created with the eXpress Config utility on the desktop/laptop computer, not the mobile device. Depending on the bar code length and the number of parameters selected, eXpress Config generates one or more bar codes for device configuration. The bar codes contain configuration parameters for the wireless client in the mobile device and may also specify the address of the Mobile Device Server.

Bar codes should be printed at a minimum of 600 dpi.

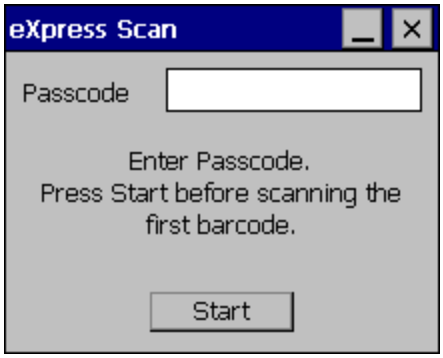
Please see *Using Wavelink Avalanche* for details on creating barcodes.

Step 2: Scan Bar Codes

For each mobile device to be configured, please follow these instructions.

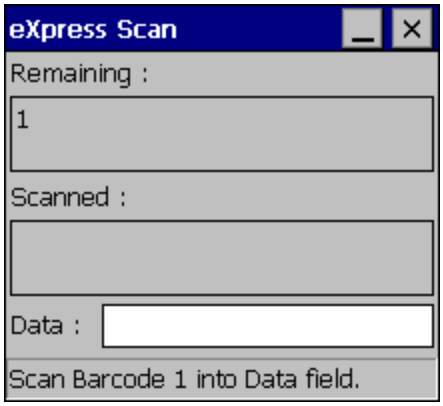
Start eXpress Scan on the VX7 by double clicking the eXpress Scan icon.

Enter the bar code password, if any.



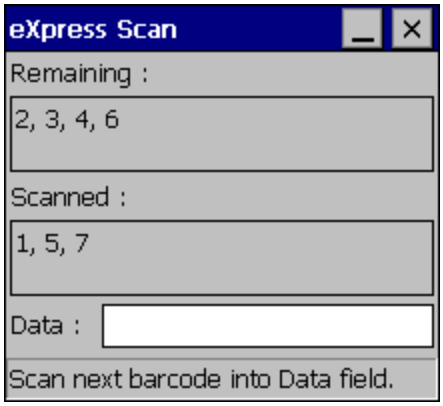
Click Start.

Bar code 1 must be scanned first. The scanned data is displayed in the “Data” text box. The password, if any, entered above is compared to the password entered when the bar codes were created.



If the passwords match, the bar code data is processed and the screen is updated to reflect the number of bar codes included in the set.

If the passwords do not match, an error message is displayed. The current screen can be closed using the X box in the upper right corner. The password can be re-entered and Bar Code 1 scanned again.



The remaining bar codes may be scanned in any order. After a bar code is scanned, that bar code is removed from the “Remaining:” list and placed in the “Scanned:” list.

Step 3: Process Completion

After the last bar code is scanned, the settings are automatically applied.

Once configured, the VX7 is warmbooted. Once connected to the wireless network and the Mobile Device Server, any software updates and additional configuration data are downloaded.

Chapter 5: Wireless Network Configuration

The radio can be configured for no encryption, WEP encryption or WPA security.

Security Options Supported are

- None
- WEP
- LEAP
- WPA-PSK
- WPA/LEAP
- PEAP-MSCHAP
- PEAP-GTC
- EAP-TLS
- EAP-FAST

Important Notes

	It is important that all dates are correct on the VX7 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.
	It may be necessary to upgrade radio software in order to use certain Summit Client Utility (SCU) features. Contact Technical Assistance for details.
	When using the 802.11a radio, the U-NII 1 band is the preferred band for indoor operation. For regulatory domains in which the U-NII 3 band is allowed, the following channels are supported: 149, 157 and 161. The AP must be configured accordingly.

After making any changes to the wireless configuration, warmboot the VX7.

Summit Client Utility

Note: When making changes to profile or global parameters, the device should be warmbooted afterwards.

Start > Programs > Summit > SCU ***or***

SCU Icon on Desktop ***or***

Summit Tray Icon (if present) ***or***

Wi-FI Icon in the Windows Control Panel (if present)

The Main Tab provides information, admin login and active profile selection.

Profile specific parameters are found on the Profile Tab. The parameters on this tab can be set to unique values for each profile. This tab was labeled Config in early versions of the SCU.

The Status Tab contains information on the current connection.

The Diags Tab provides utilities to troubleshoot the radio.

Global parameters are found on the Global Tab. The values for these parameters apply to all profiles. This tab was labeled Global Settings in early versions of the SCU.

Help

Help is available by clicking the ? icon in the title bar on most SCU screens.

The SCU help may also be accessed by selecting **Start > Help** and tapping the Summit Client Utility link. The SCU does not have to be accessed to view the help information using this option.

Summit Tray Icon

The Summit tray icon provides access to the SCU and is a visual indicator of radio status.

The Summit tray icon is displayed when:

- The Summit radio is installed and active
- The Windows Zero Config utility is not active
- The Tray Icon setting is On

Click the icon to launch the SCU. Use the tray icon to view the radio status:

	The radio is not currently associated or authenticated to an Access Point
	The signal strength for the currently associated/authenticated Access Point is less than -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -71 dBm to -90 dBm
	The signal strength for the currently associated/authenticated Access Point is -51 dBm to -70 dBm
	The signal strength for the currently associated/authenticated Access Point is greater than -50 dBm

Wireless Zero Config Utility and the Summit Radio

- The WZC utility has an icon in the toolbar that looks like networked computers with a red X through them, indicating that Wireless Zero Config application is enabled but the connection is inactive at this time (the device is not connected to a network). The WZC icon may not be visible until control is passed to the WZC utility as described below.
- You can use either the Wireless Zero Configuration Utility or the Summit Client Utility to connect to your network. As the Wireless Zero Configuration Utility cannot control the complete set of security features of the radio, it is recommended to use the Summit Client Utility to connect to your network.

How To: Use the Wireless Zero Config Utility

1. Select **ThirdPartyConfig** in the Active Profile drop down list as the active profile (see Main Tab).
2. Warmboot the device.

The Summit Client Utility passes control to Wireless Zero Config and the WZC Wireless Information control panel. Using the options in the Wireless Zero Config panels, setup radio and security settings. There may be a slight delay before the Wireless Zero Config icon indicates the status of the connection.

How to: Switch Control to SCU

1. To switch back to SCU control, select any other profile in the SCU Active Config drop down list, except **ThirdPartyConfig**.
2. Warmboot the device.

Radio control is passed to the SCU.

Main Tab

Start > Programs > Summit > Main tab

Factory Default Settings

Admin Login	SUMMIT
Radio	Enabled
Active Config/Profile	Default
Regulatory Domain	FCC or ETSI

The Main tab displays information about the wireless client device including:

- SCU (Summit Client Utility) version
- Driver version
- Radio Type (BG is an 802.11 b/g radio, ABG is an 802.11 a/b/g radio).
- Regulatory Domain
- Copyright Information can be accessed by tapping the About SCU button
- Active Config profile / Active Profile name
- Status of the client (Down, Associated, Authenticated, etc.).

The **Active Profile** can be switched without logging in to Admin mode. Selecting a different profile from the drop down list does not require logging in to Administrator mode. The profile must already exist. Perform a Suspend/Resume function when changing profiles. Profiles can be created or edited after the Admin login password has been entered and accepted.

When the profile named “ThirdPartyConfig” is chosen as the active profile, the Summit Client Utility passes control to Windows Zero Config for configuration of all client and security settings for the network module.

The **Disable Radio** button can be used to disable the network card. Once disabled, the button label changes to Enable Radio. By default the radio is enabled.

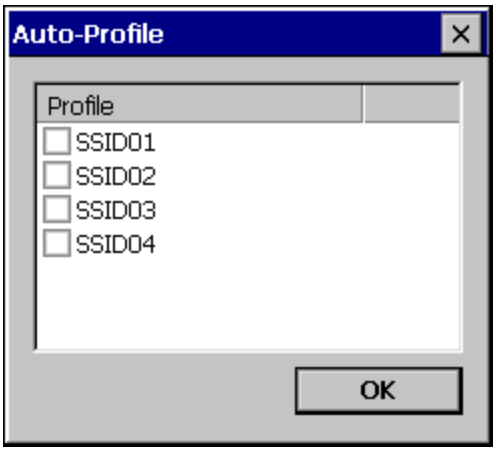
The **Admin Login** button provides access to editing wireless parameters. Profile and Global may only be edited after entering the Admin Login password.

The password is case-sensitive.

Once logged in, the button label changes to Admin Logout. To logout, either tap the **Admin Logout** button or exit the SCU without tapping the **Admin Logout** button.

Auto Profile

Auto Profile allows the user to configure a list of profiles that the SCU can search when a radio connection is lost. After using the Profile tab to create any desired profiles, return to the Main tab. To specify which profiles are to be included in Auto Profile, click the **List** button.



The Auto Profile selection screen displays all currently configured profiles. Click on the checkbox for any profiles that are to be included in Auto Profile selection then click ok to save.

To enable Auto Profile, click the **On** button on the **Main** tab.

When Auto Profile is On, if the radio goes out of range from the currently selected profile, the radio then begins to attempt to connect to the profiles listed under Auto Profile.

The search continues until:

- the SCU connects to and, if necessary, authenticates with, one of the specified profiles or
- the Off button is clicked to turn off Auto Profile.

Note: Do not include any profiles with an Ad Hoc Radio Mode in this listing.

Admin Login

To login to Administrator mode, tap the **Admin Login** button.

Once logged in, the button label changes to Admin Logout. The admin is automatically logged out when the SCU is exited. The Admin can either tap the **Admin Logout** button, or the **OK** button to logout. The Administrator remains logged in when the SCU is not closed and a Suspend/Resume function is performed.

Enter the Admin password (the default password is SUMMIT and is case sensitive) and tap **OK**. If the password is incorrect, an error message is displayed.

The Administrator default password can be changed on the Global tab.

The end-user can:

- Turn the radio on or off on the Main tab.
- Select an active Profile on the Main tab.
- View the current parameter settings for the profiles on the Profile tab.
- View the global parameter settings on the Global tab.
- View the current connection details on the Status tab.
- View radio status, software versions and regulatory domain on the Main tab.
- Access additional troubleshooting features on the Diags tab.

After Admin Login, the end-user can also:

- Create, edit, rename and delete profiles on the Profile tab.
- Edit global parameters on the Global tab.
- Enable/disable the Summit tray icon in the taskbar.

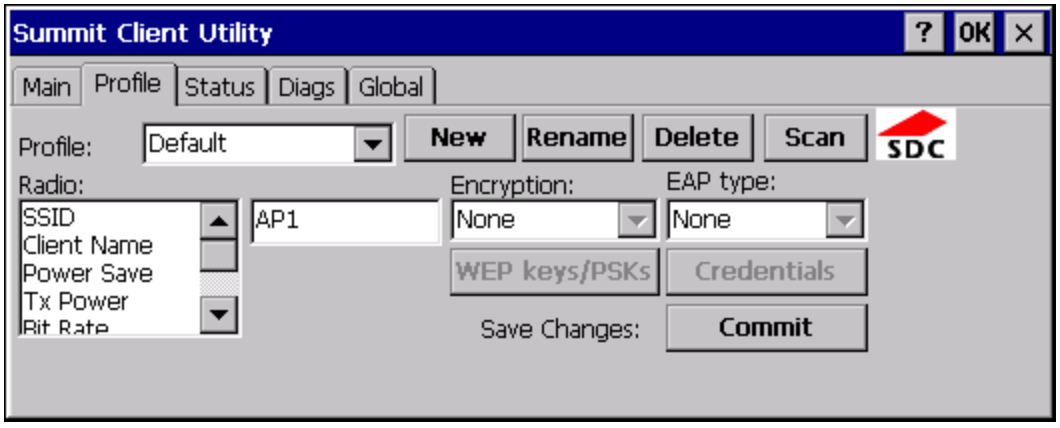
Profile Tab

Start > Programs > Summit > Profile tab

Note: Tap the Commit button to save changes before leaving this panel or the SCU. If the panel is exited before tapping the Commit button, changes are not saved!

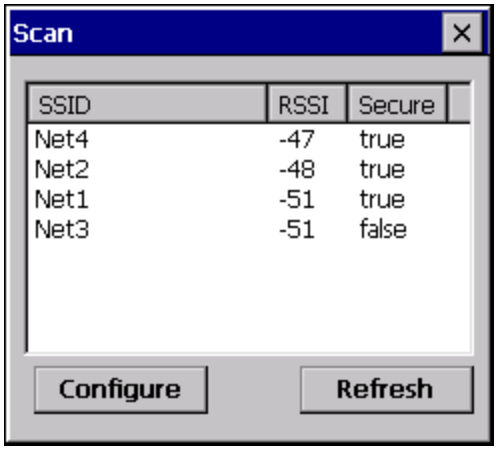
Factory Default Settings

Profile	Default
SSID	Blank
Client Name	Blank
Power Save	CAM
Tx Power	Maximum
Bit Rate	Auto
Radio Mode	See Profile Parameters for default
Auth Type	Open
EAP Type	None
Encryption	None



When logged in as an Admin (see Admin Login), use the Profile tab to manage profiles. When not logged in as an Admin, the parameters can be viewed, and cannot be changed. The buttons on this tab are dimmed if the user is not logged in as Admin. The Profile tab was previously labeled Config.

Buttons

Button	Function
Commit	Saves the profile settings made on this screen. Settings are saved in the profile.
Credentials	Allows entry of a username and password, certificate names, and other information required to authenticate with the access point. The information required depends on the EAP type.
Delete	Deletes the profile. The current active profile cannot be deleted and an error message is displayed if a delete is attempted.
New	Creates a new profile with the default settings (see Profile Parameters) and prompts for a unique name. If the name is not unique, an error message is displayed and the new profile is not created.
Rename	Assigns a new, unique name. If the new name is not unique, an error message is displayed and the profile is not renamed.
Scan	Opens a window that lists access points that are broadcasting their SSIDs. Tap the Refresh button to view an updated list of APs. Each AP's SSID, its received signal strength indication (RSSI) and whether or not data encryption is in use (true or false). Sort the list by tapping on the column headers. If the scan finds more than one AP with the same SSID, the list displays the AP with the strongest RSSI and the least security.  If you are logged in as an Admin, tap an SSID in the list and tap the Configure button, you return to the Profile window to recreate a profile for that SSID, with the profile name being the same as the SSID (or the SSID with a suffix such as "_1" if a profile with the SSID as its name exists already).
WEP Keys / PSK Keys	Allows entry of WEP keys or pass phrase as required by the type of encryption.

Note: Unsaved Changes – The SCU will display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from this tab.

The settings for Auth Type, EAP Type and Encryption depend on the security type chosen.

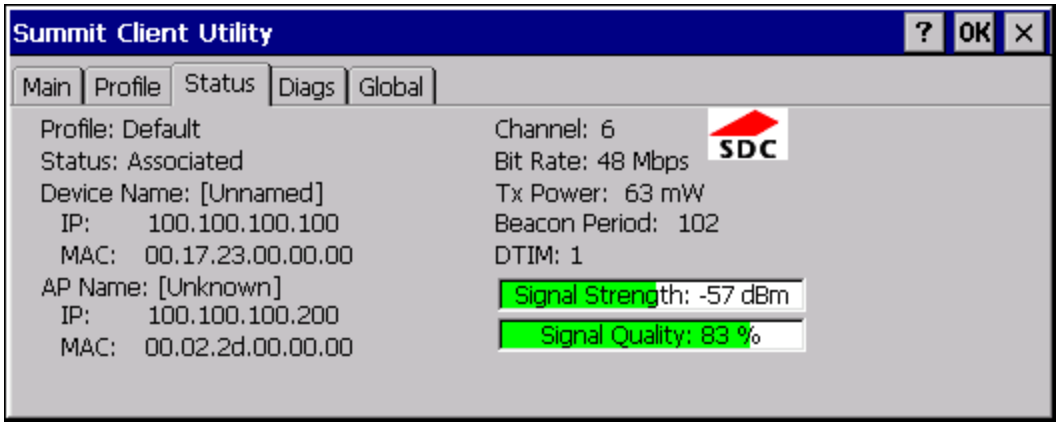
Profile Parameters

Parameter	Default	Explanation
Edit Profile	Default	A string of 1 to 32 alphanumeric characters, establishes the name of the Profile. Options are Default or ThirdPartyConfig.
SSID	Blank	A string of up to 32 alphanumeric characters. Establishes the Service Set Identifier (SSID) of the WLAN to which the client connects.
Client Name	Blank	A string of up to 16 characters. The client name is assigned to the network card and the device using the network card. The client name may be passed to networking wireless devices, e.g. Access Points.
Power Save	CAM	Power save mode. Options are: Constantly Awake Mode (CAM) power save off, Maximum (power saving mode) and Fast (power saving mode). When using power management, use FAST for best throughput results.
Tx Power	Maximum	Maximum setting regulates Tx power according to the Max power setting for the current regulatory domain. Options are: Maximum, 50mW, 30mW, 20mW, 10mW, 5mW, or 1mW.
Bit Rate	Auto	Setting the rate to Auto will allow the Access Point to automatically negotiate the bit rate with the client device. Options are: Auto, 1 Mbit, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit.
Auth Type	Open	802.11 authentication type used when associating with the Access Point. Options are: Open, LEAP, or Shared key.
EAP Type	None	Extensible Authentication Protocol (EAP) type used for 802.1x authentication to the Access Point. Options are: None, LEAP, EAP-FAST, PEAP-MSCHAP, PEAP-GTC, PEAP-TLS, EAP-TTLS, or EAP-TLS. EAP Type chosen determines whether the Credentials button is active and also determines the available entries in the Credentials pop-up window.
Encryption	None	Type of encryption to be used to protect transmitted data. Available options may vary by SCU version. Options are: None, WEP(or Manual WEP), WEP EAP (or Auto WEP), WPA PSK, WPA TKIP, WPA CCKM, WPA2 PSK, WPA2 AES, or WPA2 CCKM. CKIP is not supported in the VX7. The Encryption type chosen determines if the WEP Keys / PSK Keys button is active and also determines the available entries in the WEP or PSK pop-up window.

<table>
<tr><th>Parameter</th><th>Default</th><th>Explanation</th></tr>
<tr><td>Radio Mode</td><td>BG radio:
BG Rates Full
Or
A radio:
BGA Rates Full</td><td>Specify 802.11a, 802.11b and/or 802.11g rates when communicating with the AP. The options displayed for this parameter depend on the type of radio (802.11b/g or 802.11a/b/g)installed in the mobile device.
Options:
B rates only (1, 2, 5.5 and 11 Mbps)
BG Rates Full (All B and G rates)
G rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps)
BG optimized or BG subset (1, 2, 5.5, 6, 11, 24, 36 and 54 Mbps)
A rates only (6, 9, 12, 18, 24, 36, 48 and 54 Mbps)
ABG Rates Full (All A rates and all B and G rates with A rates preferred)
BGA Rates Full (All B and G rates and all A rates with B and G rates preferred)
Ad Hoc (when connecting to another client device instead of an AP)
Default:
BG Rates Full (for 802.11b/g radios)
BGA Rates Full (for 802.11a/b/g radio)
BG radio only – Previous SCU versions may have the default set as BG Rates Full. Depending on the SCU version, either BG Optimized or BG subset is the default.
It is important the Radio Mode parameter correspond to the AP to which the device is to connect. For example, if this parameter is set to G rates only, the VX7 may only connect to APs set for G rates and not those set for B and G rates.
The options for the Radio Mode parameter should be set, based on the antenna configuration, as follows:
<table><tr><th>Antenna Configuration</th><th>Radio Mode</th></tr><tr><td>A Main and BG Main</td><td>ABG Rates Full
BGA Rates Full</td></tr><tr><td>A Main and A Aux</td><td>A Rates Only</td></tr><tr><td>BG Main and BG Aux</td><td>B Rates Only
G Rates Only
BG Rates Full
BG Subset</td></tr><tr><td>A Main only</td><td>A Rates Only</td></tr><tr><td>BG Main only</td><td>B Rates Only
G Rates Only
BG Rates Full
BG Rates Subset</td></tr></table>
Contact Technical Assistance if you have questions about the antenna(s) installed on your VX7.</td></tr>
</table>

Status Tab

Start > Programs > Summit > Status tab



This screen provides information on the radio:

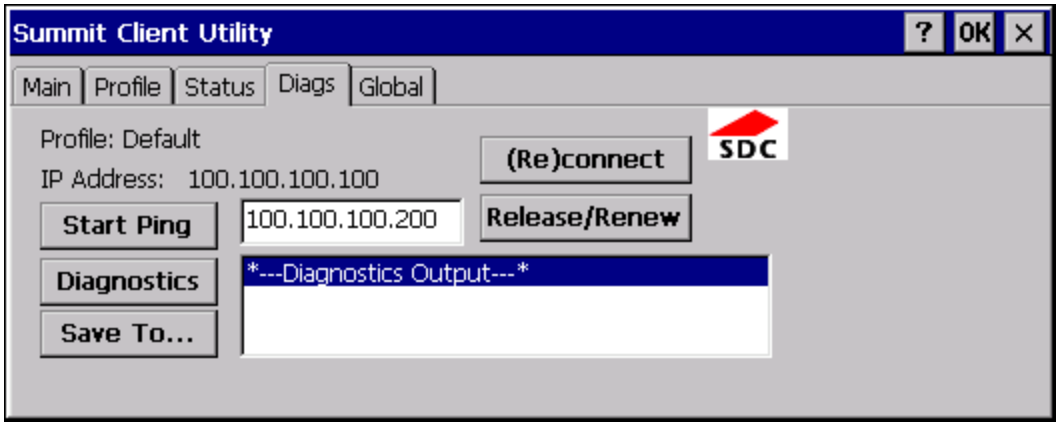
- The profile being used.
- The status of the radio card (down, associated, authenticated, etc.).
- Client information including device name, IP address and MAC address.
- Information about the Access Point (AP) maintaining the connection to the network including AP name, IP address and MAC address.
- Channel currently being used for wireless traffic.
- Bit rate in Mbit.
- Current transmit power in mW.
- Beacon period – the time between AP beacons in kilomicroseconds. (one kilomicrosecond = 1,024 microseconds).
- DTIM interval – A multiple of the beacon period that specifies how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power saving devices a packet is waiting for them. For example, if DTIM = 3, then every third beacon contains a DTIM.
- Signal strength (RSSI) displayed in dBm and graphically.
- Signal quality, a measure of the clarity of the signal displayed in percentage and graphically.

There are no user entries on this screen.

Note: After completing radio configuration, it is a good idea to review this screen to verify the radio has associated (no encryption, WEP) or authenticated (LEAP, any WPA), as indicated above.

Diags Tab

Start > Programs > Summit > Diags tab



The Diags screen can be used for troubleshooting network traffic and radio connectivity issues.

- **(Re)connect** – Use this button to apply (or reapply) the current profile and attempt to associate or authenticate to the wireless LAN. All activity is logged in the Diagnostic Output box on the lower part of the screen.
- **Release/Renew** – Obtain a new IP address through release and renew. All activity is logged in the Diagnostic Output box. If a fixed IP address has been assigned to the radio, this is also noted in the Diagnostic Output box. Note that the current IP address is displayed above this button.
- **Start Ping** – Start a continuous ping to the IP address specified in the text box to the right of this button. Once the button is clicked, the ping begins and the button label changes to **Stop Ping**. Clicking the button ends the ping. The ping also ends when any other button on this screen is clicked or the user browses away from the Diags tab. The results of the ping are displayed in the Diagnostic Output box.
- **Diagnostics** – Also attempts to (re)connect to the wireless LAN. However, this option provides more data in the Diagnostic Output box than the (Re)connect option. This data dump includes radio state, profile settings, global settings, and a list of broadcast SSID APs.
- **Save To…** – Use this to save the results of the diagnostics to a text file. Use the explorer window to specify the name and location for the diagnostic file. The text file can viewed using an application such as WordPad.

Global Tab

Start > Programs > Summit > Global tab

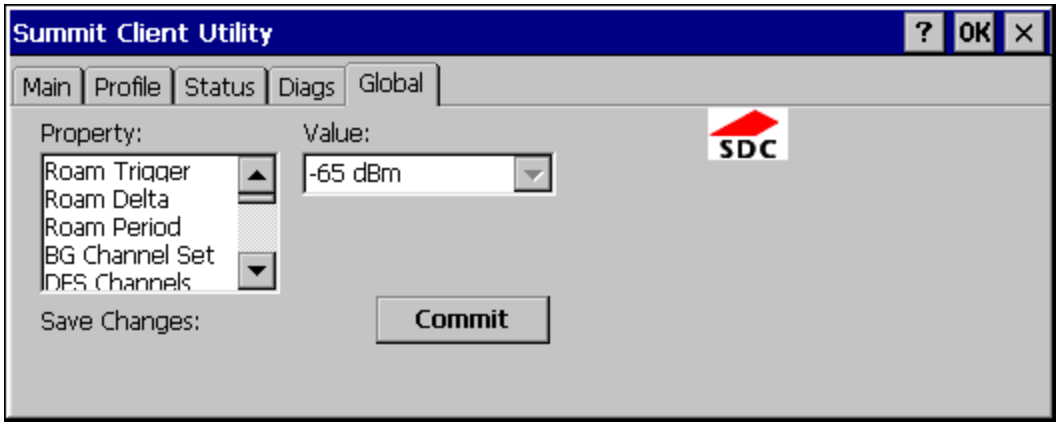
The parameters on this panel can only be changed when an Admin is logged in with a password. The current values for the parameters can be viewed by the general user without requiring a password.

Note: Tap the Commit button to save changes. If the panel is exited before tapping the Commit button, changes are not saved!

Factory Default Settings

Roam Trigger	-65 dBm
Roam Delta	5 dBm
Roam Period	BG: 10 sec. A: 5 sec.
BG Channel Set	Full
DFS Channels	Off
Ad Hoc Channel	1
Aggressive Scan	On
CCX Features	BG: Off A: Optimized
WMM	Off
Auth Server	Type 1
TTLS Inner Method	Auto-EAP
PMK Caching	Standard
WAPI	Off (dimmed)
TX Diversity	BG: On A: Main Only
RX Diversity	BG: On-Start on Main A: Main Only
Frag Threshold	2346
RTS Threshold	2347
LED	Off
Tray Icon	On
Hide Passwords	On
Admin Password	SUMMIT (or blank)
Auth Timeout	8 seconds
Certs Path	System
Ping Payload	32 bytes

Ping Timeout	5000 ms
Ping Delay ms	1000 ms



Custom Parameter Option

Honeywell does not support the parameter Custom option. The parameter value is displayed as “Custom” when the operating system registry has been edited to set the Summit parameter to a value that is not available from the parameter’s drop down list. Selecting Custom from the drop down list has no effect. Selecting any other value from the drop down list will overwrite the “custom” value in the registry.

Global Parameters

Parameter	Default	Function
Roam Trigger	-65 dBm	If signal strength is less than this trigger value, the client looks for a different Access Point with a stronger signal. Options are: -50 dBm, -55, -60, -65, -70, -75, -80, -85, -90 dBm or Custom. Available options may vary by SCU revision.
Roam Delta	5 dBm	The amount by which a different Access Point signal strength must exceed the current Access Point signal strength before roaming to the different Access Point is attempted. Options are: 5 dBm, 10, 15, 20, 25, 30, 35 dBm or Custom. Roam delta dBm may vary by SCU revision.
Roam Period	BG: 10 sec. A: 5 sec.	The amount of time, after association or a roam scan with no roam, that the radio collects Received Signal Strength Indication (RSSI) scan data before a roaming decision is made. Options are: 5 sec, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60 seconds or Custom.
BG Channel Set	Full	Defines the 2.4GHz channels to be scanned for an AP when the radio is contemplating roaming. By specifying the channels to search, roaming time may be reduced over scanning all channels. Options are: Full (all channels) 1,6,11 (the most commonly used channels) 1,7,13 (for ETSI and TELEC radios only) Custom.
DFS Channels	Off	Support for 5GHZ 802.11a channels where support for DFS is required. Options are: On, Off, Optimized. Not supported (always off) in some releases.
Ad Hoc Channel	1	Use this parameter when the Radio Mode profile parameter is set to Ad Hoc. Specifies the channel to be used for an Ad Hoc connection to another client device. If a channel is selected that is not supported by the by the radio, the default value is used. Options are: 1 through 14 (the 2.4GHz channels) 36, 40, 44, 48 (the UNII-1 channels)
Aggressive Scan	On	When set to On and the current connection to an AP weakens, the radio aggressively scans for available APs. Aggressive scanning works with standard scanning (set through Roam Trigger, Roam Delta and Roam Period). Aggressive scanning should be set to On unless there is significant co-channel interference due to overlapping APs on the same channel. Options are: On, Off

Parameter	Default	Function
CCX or CCX Features	BG: Off A: Optimized	Use of Cisco Compatible Extensions (CCX) radio management and AP specified maximum transmit power features. Options are: Full - Use Cisco IE and CCX version number, support all CCX features. The option known as "On" in previous versions. Optimized –Use Cisco IE and CCX version number, support all CCX features except AP assisted roaming, AP specified maximum transmit power and radio management. Off - Do not use Cisco IE and CCX version number. Cisco IE = Cisco Information Element.
WMM	Off	Use of Wi-Fi Multimedia extensions. Options are: On, Off Devices running Windows XP can change the default value. Devices running all other OS cannot change the default value.
Auth Server	Type 1	Specifies the type of authentication server. Options are: Type 1 (ACS server) and Type 2 (non-ACS server)
TTLS Inner Method	Auto-EAP	Authentication method used within the secure tunnel created by EAP-TTLS. Options are: AUTO-EAP (Any available EAP method) MSCHAPV2 MSCHAP PAP CHAP EAP-MSCHAPV2
PMK Caching	Standard	Type of Pairwise Master Key (PMK) caching to use when WPA2 is in use. PMK caching is designed to speed up roaming between APs by allowing the client and the AP to cache the results of 802.1X authentications, eliminating the need to communicate with the ACS server. Standard PMK is used when there are no controllers. The reauthentication information is cached on the original AP. The client and the AP use the cached information to perform the four-way handshake to exchange keys. Opportunistic PMK (OPMK) is used when there are controllers. The reauthentication information cached on the controllers. The client and the controller behind the AP use the cached information to perform the four-way handshake to exchange keys. If the selected PMK caching method is not supported by the network infrastructure, every roam requires full 802.11X authentication, including interaction with the ACS server. If the active profile is using WPA2 CCKM, the global PMK Caching setting is ignored and the client attempts to use CCKM. Options are: Standard, OPMK This change does not take effect until after a Suspend/Resume cycle.
WAPI	Off	Default is Off and dimmed (cannot be changed).

<table>
<tr><th>Parameter</th><th>Default</th><th>Function</th></tr>
<tr><td>TX Diversity</td><td>BG: On
A: Main Only</td><td>How to handle antenna diversity when transmitting packets to the Access Point.
Options are:
Main only (use the main antenna only)
Aux only (use the auxiliary antenna only)
On (use diversity or both antennas).
The options for the TX Diversity parameter should be set, based on the antenna configuration, as follows:
<table><tr><th>Antenna Configuration</th><th>TX Diversity</th></tr><tr><td>A Main and BG Main</td><td>Main Only</td></tr><tr><td>A Main and A Aux</td><td>On</td></tr><tr><td>BG Main and BG Aux</td><td>On</td></tr><tr><td>A Main only</td><td>Main Only</td></tr><tr><td>BG Main only</td><td>Main Only</td></tr></table>
Contact Technical Assistance if you have questions about the antenna(s) installed on your VX7.</td></tr>
<tr><td>RX Diversity</td><td>BG: On-Start on Main
A: Main Only</td><td>How to handle antenna diversity when receiving packets from the Access Point.
Options are:
Main Only (use the main antenna only)
Aux Only (use the auxiliary antenna only)
On-start on Main (on startup, use the main antenna)
On-start on Aux (on startup, use the auxiliary antenna).
The options for the RX Diversity parameter should be set, based on the antenna configuration, as follows:
<table><tr><th>Antenna Configuration</th><th>RX Diversity</th></tr><tr><td>A Main and BG Main</td><td>Main Only</td></tr><tr><td>A Main and A Aux</td><td>On-start on Main</td></tr><tr><td>BG Main and BG Aux</td><td>On-start on Main</td></tr><tr><td>A Main only</td><td>Main Only</td></tr><tr><td>BG Main only</td><td>Main Only</td></tr></table>
Contact Technical Assistance if you have questions about the antenna(s) installed on your VX7.</td></tr>
<tr><td>Frag Thresh</td><td>2346</td><td>If the packet size (in bytes) exceeds the specified number of bytes set in the fragment threshold, the packet is fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of wireless interference.
Options are: Any number between 256 bytes and 2346 bytes.</td></tr>
</table>

Parameter	Default	Function
RTS Thresh	2347	If the packet size exceeds the specified number of bytes set in the Request to Send (RTS) threshold, an RTS is sent before sending the packet. A low RTS threshold setting can be useful in areas where many client devices are associating with the Access Point. Options are: Any number between 0 and 2347.
LED	Off	The LED on the wireless card is not visible to the user when the wireless card is installed in a sealed mobile device. Options are: On, Off.
Tray Icon	On	Determines if the Summit icon is displayed in the System tray. Options are: On, Off
Hide Password	On	When On, the Summit Config Utility masks passwords (characters on the screen are displayed as an *) as they are typed and when they are viewed. When Off, password characters are not masked. Options are: On, Off.
Admin Password	SUMMIT(or Blank)	A string of up to 64 alphanumeric characters that must be entered when the Admin Login button is tapped. If Hide Password is On, the password is masked when typed in the Admin Password Entry dialog box. The password is case sensitive. This value is masked when the Admin is logged out. Options are: none.
Auth Timeout	8 seconds	Specifies the number of seconds the Summit software waits for an EAP authentication request to succeed or fail. If the authentication credentials are stored in the active profile and the authentication times out, the association fails. No error message or prompting for corrected credentials is displayed. If the authentication credentials are not stored in the active profile and the authentication times out, the user is again prompted to enter the credentials. Options are: An integer from 3 to 60.
Certs Path	System	A valid directory path, of up to 64 characters, where WPA Certificate Authority and User Certificates are stored on the mobile device when not using the Windows certificates store. Ensure the Windows folder path currently exists before assigning the path in this parameter. See Certificates for instructions on obtaining CA and User Certificates. Options are: none. For example, when the valid certificate is stored as My Computer/System/MYCERTIFICATE.CER, enter System in the Certs Path text box as the Windows folder path.
Ping Payload	32 bytes	Maximum amount of data to be transmitted on a ping. Options are: 32 bytes, 64, 128, 256, 512, or 1024 bytes.
Ping Timeout ms	5000	The amount of time, in milliseconds, that a device will be continuously pinged. The Stop Ping button can be tapped to end the ping process ahead of the ping timeout. Options are: Any number between 0 and 30000 ms.
Ping Delay ms	1000	The amount of time, in milliseconds, between each ping after a Start Ping button tap. Options are: Any number between 0 and 30000 ms.

Note: Tap the Commit button to save changes. If this panel is closed before tapping the Commit button, changes are not saved!

Sign-On vs. Stored Credentials

When using wireless security that requires a user name and password to be entered, the Summit Client Utility offers these choices:

- The Username and Password may be entered on the Credentials screen. If this method is selected, anyone using the device can access the network.
- The Username and Password are left blank on the Credentials screen. When the device attempts to connect to the network, a sign on screen is displayed. The user must enter the Username and Password at that time to authenticate.

How to: Use Stored Credentials

1. After completing the other entries in the profile, click on the **Credentials** button.
2. Enter the Username and Password on the Credentials screen and click the **OK** button.
3. Click the **Commit** button.
4. For LEAP and WPA/LEAP, configuration is complete.
5. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
6. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
7. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.
8. The default is to use the entire certificate store for the CA certificate. Alternatively, use the **Browse** button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
9. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
10. If using EAP FAST and manual PAC provisioning, input the PAC filename and password..
11. Click the **OK** button then the **Commit** button.
12. If changes are made to the stored credentials, click **Commit** to save those changes before making any additional changes to the profile or global parameters.
13. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status tab indicates the device is Authenticated and the method used.

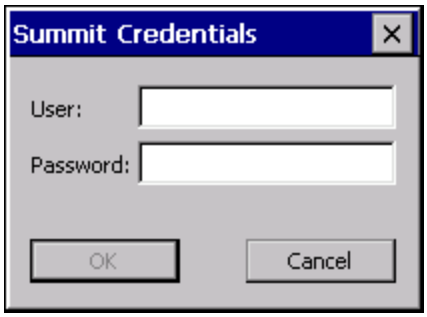
Note: See Configuring the Profile for more details.

Note: If invalid credentials are entered into the stored credentials, the authentication will fail. No error message is displayed. The user may or may not be prompted to enter valid credentials.

How to: Use Sign On Screen

1. After completing the other entries in the profile, click on the **Credentials** button. Leave the Username and Password blank. No entries are necessary on the Credentials screen for LEAP or LEAP/WPA.
2. For PEAP-MSCHAP and PEAP-GTC, importing the CA certificate into the Windows certificate store is optional.
3. For EAP-TLS, import the CA certificate into the Windows certificate store. Also import the User Certificate into the Windows certificate store.
4. Access the Credentials screen again. Make sure the **Validate server** and **Use MS store** checkboxes are checked.

5. The default is to use the entire certificate store for the CA certificate. Alternatively, use the Browse button next to the CA Cert (CA Certificate Filename) on the Credentials screen to select an individual certificate.
6. For EAP-TLS, also enter the User Cert (User Certificate filename) on the credentials screen by using the **Browse** button.
7. Click the **OK** button then the **Commit** button.
8. When the device attempts to connect to the network, a sign-on screen is displayed.
9. Enter the Username and Password. Click the **OK** button.



10. Verify the device is authenticated by reviewing the Status tab. When the device is property configured, the Status Tab indicates the device is Authenticated and the method used.
11. The sign-on screen is displayed after a reboot.

Note: See Configuring the Profile for more details.

If a user enters invalid credentials and clicks **OK**, the device associates but does not authenticate. The user is again prompted to enter credentials.

If the user clicks the **Cancel** button, the device does not associate. The user is not prompted again for credentials until:

- the device is rebooted,
- the radio is disabled then enabled,
- the **Reconnect** button on the Diags Tab is clicked or
- the profile is modified and the **Commit** button is clicked.

Windows Certificate Store vs. Certs Path

Note: It is important that all dates are correct on the VX7 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

User Certificates

EAP-TLS authentication requires a user certificate. The user certificate must be stored in the Windows certificate store.

- To generate the user certificate, see Generating a User Certificate.
- To import the user certificate into the Windows certificate store, see Installing a User Certificate.
- A Root CA certificate is also needed. Refer to the section below.

Root CA Certificates

Root CA certificates are required for EAP/TLS, PEAP/GTC and PEAP/MSCHAP. Two options are offered for storing these certificates. They may be imported into the Windows certificate store or copied into the Certs Path directory.

How To: Use the Certs Path

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. Copy the certificate to specified directory on the mobile device. The default location for Certs Path is \System. A different location may be specified by using the Certs Path global variable. Please note the location chosen for certificate storage should persist after a reboot.
3. When completing the Credentials screen for the desired authentication, do not check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. Enter the certificate name in the CA Cert textbox.
5. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

How To: Use Windows Certificate Store

1. See Generating a Root CA Certificate and follow the instructions to download the Root Certificate to a PC.
2. To import the certificate into the Windows store, See Installing a Root CA Certificate.
3. When completing the Credentials screen for the desired authentication, be sure to check the **Use MS store** checkbox after checking the **Validate server** checkbox.
4. The default is to use all certificates in the store. If this is OK, skip to the last step.
5. Otherwise, to select a specific certificate click on the **Browse (…)** button.

6. Uncheck the **Use full trusted store** checkbox.
7. Select the desired certificate and click the **Select** button to return the selected certificate to the CA Cert textbox.
8. Click **OK** to exit the Credentials screen and then **Commit** to save the profile changes.

Configuring the Profile

Use the instructions in this section to complete the entries on the Profile tab according to the type of wireless security used by your network. The instructions that follow are the minimum required to successfully connect to a network. Your system may require more parameters than are listed in these instructions. Please see your system administrator for complete information about your network and its wireless security requirements.

To begin the configuration process:

- On the Main Tab, click the Admin Login button and enter the password.
- If using a single profile, edit the default profile with the parameters for your network. Select the Default profile from the pull down menu.
- Make any desired parameter changes as described in the applicable following section determined by network security type and click the **Commit** button to save the changes.

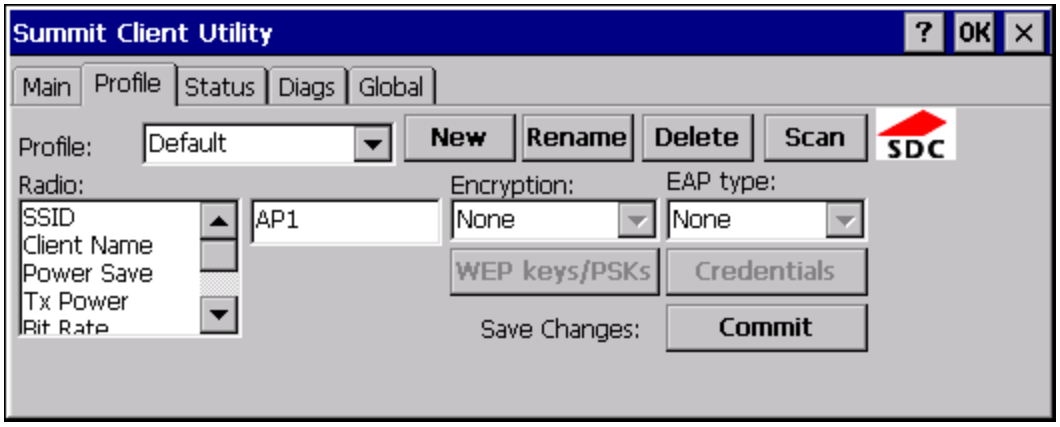
Remember to click the Commit button after making changes to ensure the changes are saved. Many versions of the SCU display a reminder if the Commit button is not clicked before an attempt is made to close or browse away from the tab in focus if there are unsaved changes.

If changes are made to the *stored credentials*, click Commit to save those changes first before making any additional changes.

No Security

To connect to a wireless network with no security, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **None**
- Set **Auth Type** to **Open**



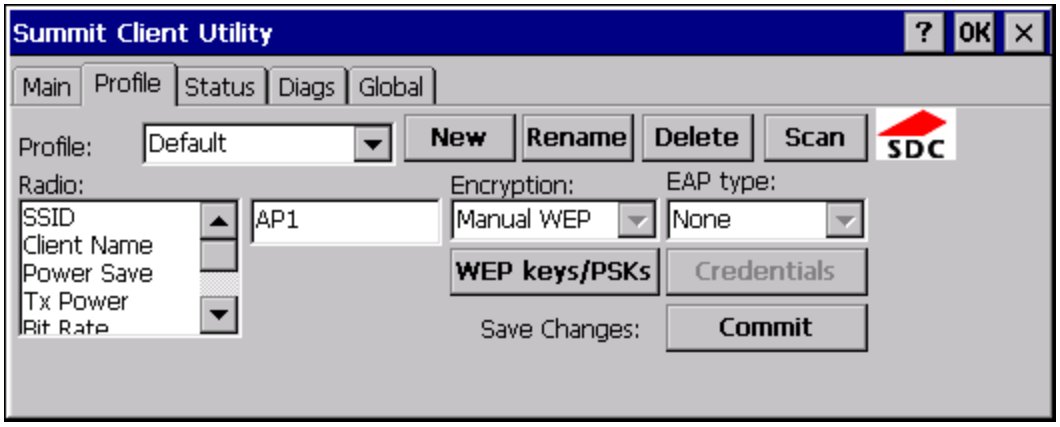
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

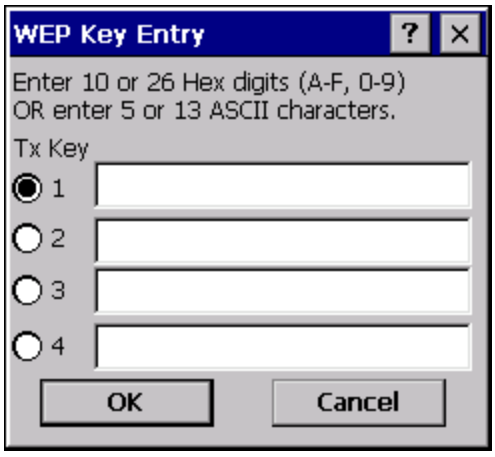
WEP

To connect using WEP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WEP** or **Manual WEP** (depending on SCU version)
- Set **Auth Type** to **Open**



Click the **WEP keys/PSKs** button.



Valid keys are 10 hexadecimal or 5 ASCII characters (for 40-bit encryption) or 26 hexadecimal or 13 ASCII characters (for 128-bit encryption). Enter the key(s) and click **OK**.

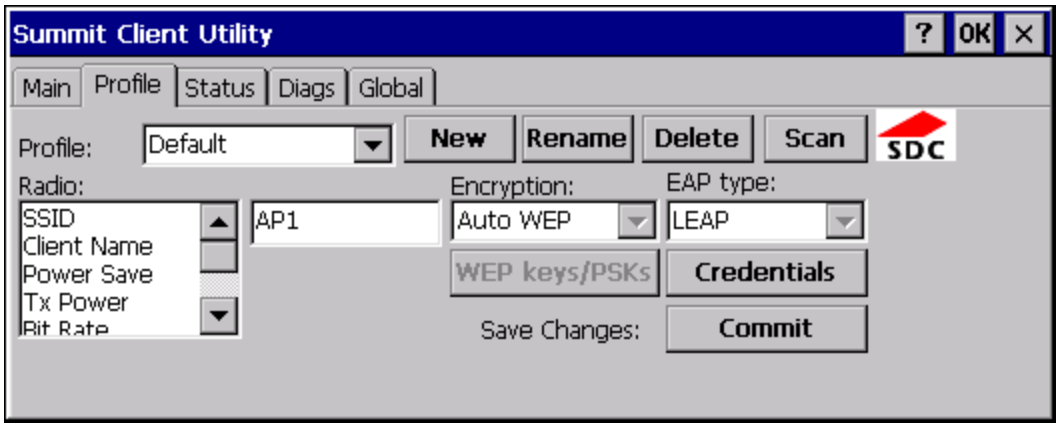
Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

LEAP

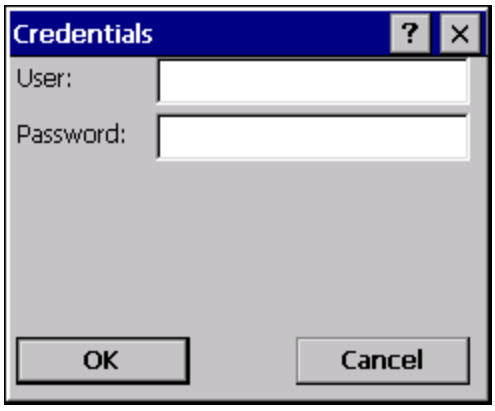
To use LEAP (without WPA), make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WEP EAP** or **Auto WEP** (depending on SCU version)
- Set **Auth Type** as follows:
    - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
    - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
    - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.



See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password. Click **OK** then click **Commit.**

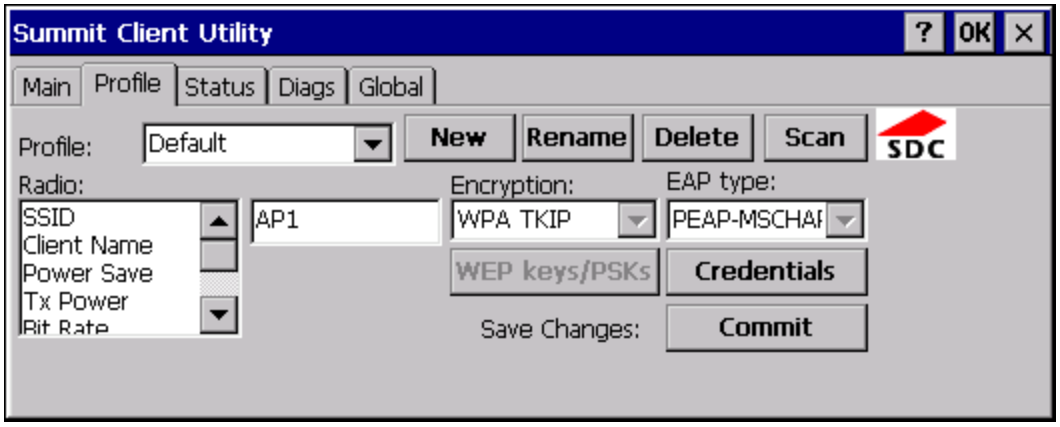
Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

PEAP/MSCHAP

To use PEAP/MSCHAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-MSCHAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

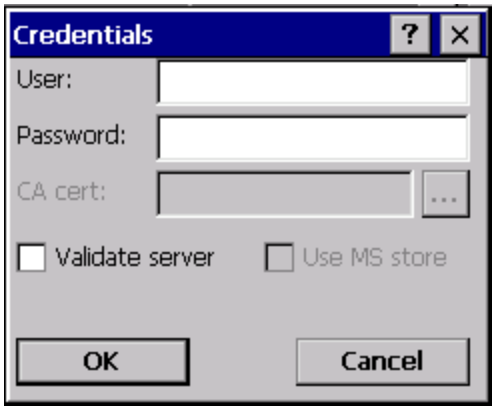


See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.
- For Stored Credentials, User, Password and the CA Certificate Filename must be entered.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

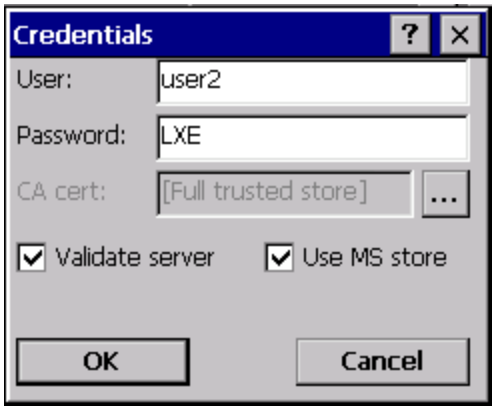
Enter the password.

Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.



If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click Select. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store** box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/MSCHAP for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

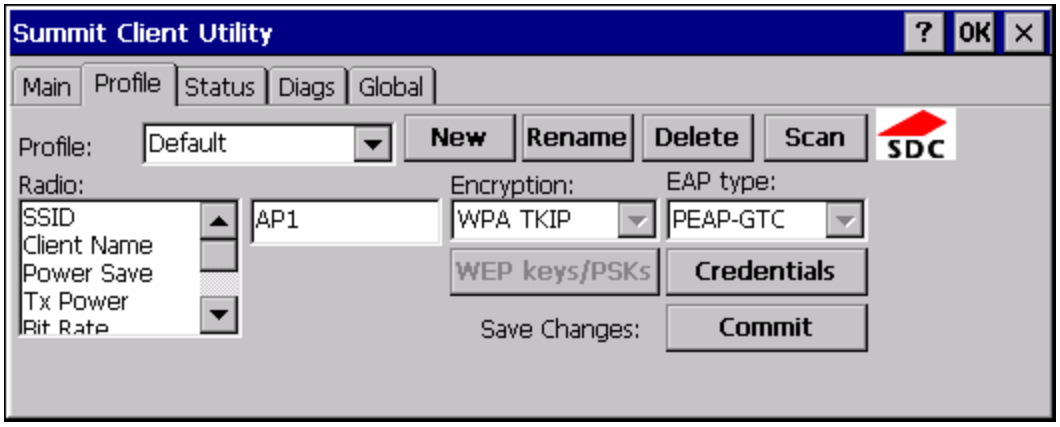
Note: The date must be properly set on the device to authenticate a certificate.

PEAP/GTC

To use PEAP/GTC, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **PEAP-GTC**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

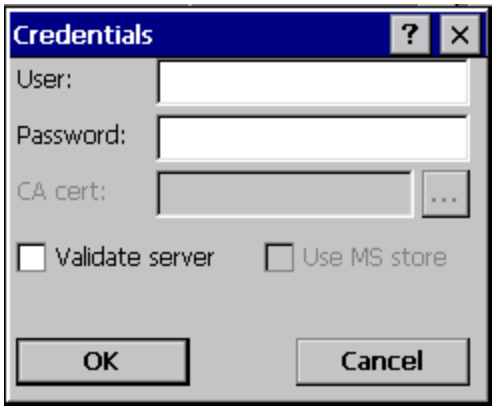


See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name and Password when connecting to the network.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

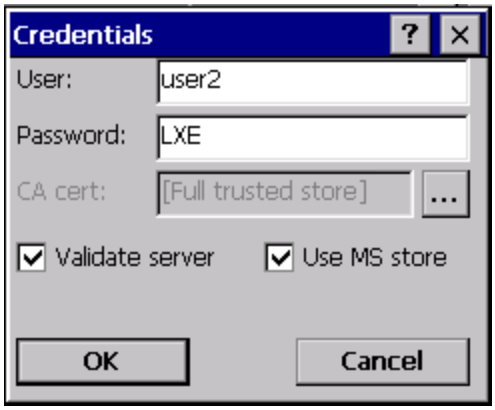
Leave the CA Certificate File Name blank for now.

Click **OK** then click **Commit**. Ensure the correct Active Profile is selected on the Main Tab.

See Windows Certificate Store vs. Certs Path for more information on certificate storage.

Once successfully authenticated, import the CA certificate into the Windows certificate store. Return to the Credentials screen and check the **Validate server** checkbox.

Note: Some servers may be configured to allow only a single use of the password for PEAP/GTC. In this case, wait for the token to update with a new password before attempting to validate the server. Then enter the new password, check the Validate Server checkbox and proceed with the certificate process below.



If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the **Use MS store box** unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The device should be authenticating the server certificate and using PEAP/GTC for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

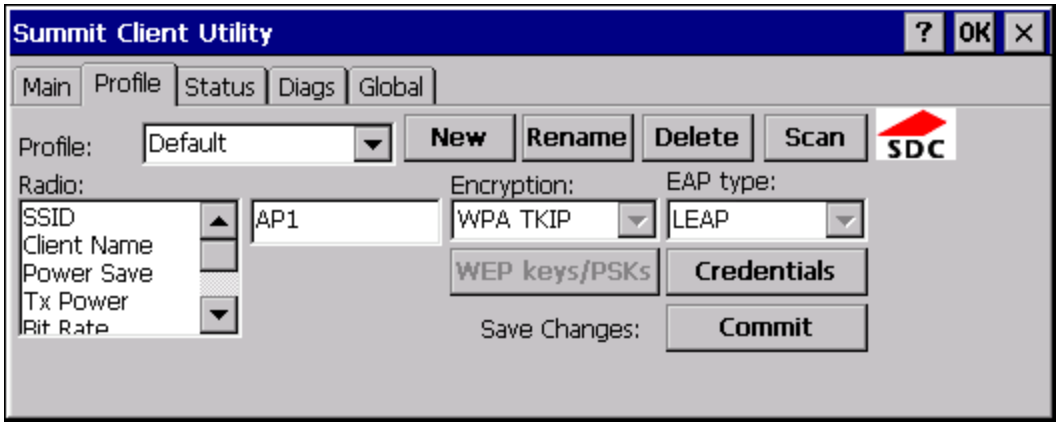
Note: The date must be properly set on the device to authenticate a certificate.

WPA/LEAP

To use WPA/LEAP, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **LEAP**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** as follows:
    - If the Cisco/CCX certified AP is configured for open authentication, set the **Auth Type** radio parameter to **Open**.
    - If the AP is configured to use shared key or passphrase, set the Auth Type radio parameter to **Shared**.
    - If the AP is configured for network EAP only, set the **Auth Type** radio parameter to **LEAP**.

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.



See Sign-On vs. Stored Credentials for information on entering credentials.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials as the user will be prompted for the Username and Password when connecting to the network.

Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Enter the password.

Click **OK** then click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

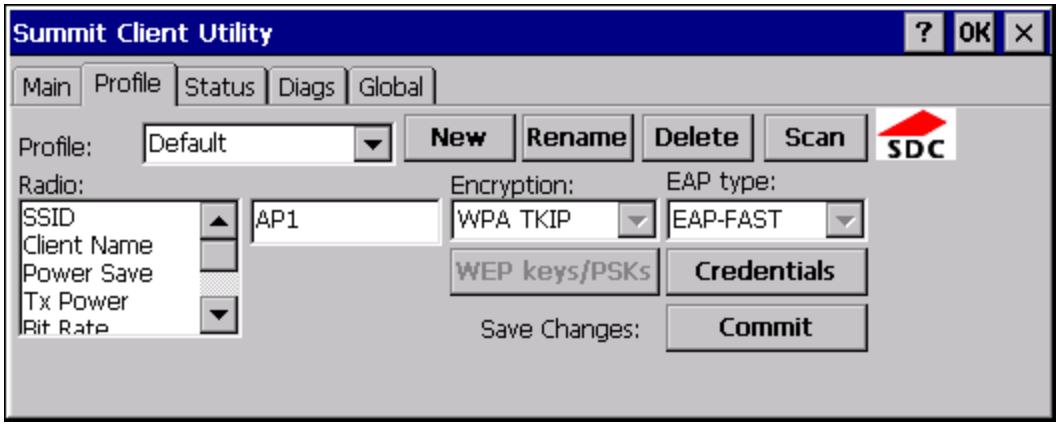
EAP-FAST

To use EAP-FAST, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-FAST**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

The SCU supports EAP-FAST with automatic or manual PAC provisioning. With automatic PAC provisioning, the user credentials, whether entered on the saved credentials screen or the sign on screen, are sent to the RADIUS server. The RADIUS server must have auto provisioning enabled to send the PAC provisioning credentials to the VX7.



For automatic PAC provisioning, once a username/password is authenticated, the PAC information is stored on the VX7. The same username/password must be used to authenticate each time. See the note below for more details.

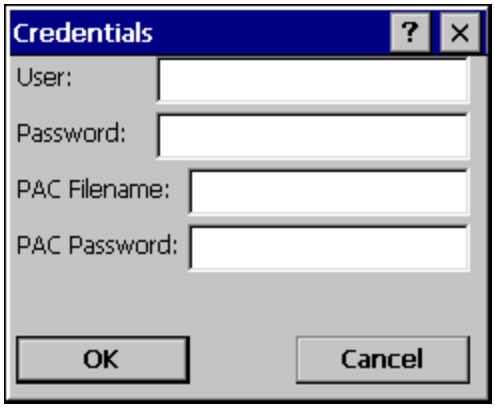
For manual PAC provisioning, the PAC filename and Password must be entered.

See Sign-On vs. Stored Credentials for information on entering credentials.

The entries on the Credentials screen are determined by the type of credentials (stored or sign on) and the type of PAC provisioning (automatic or manual).

Click on the **Credentials** button.

To use Stored Credentials, click on the **Credentials** button. No entries are necessary for Sign-On Credentials with automatic PAC provisioning as the user will be prompted for the Username and Password when connecting to the network.



To use Sign-On credentials:

- Do not enter a User and Password as the user will be prompted for the Username and Password when connecting to the network.

To use Stored Credentials:

- Enter the Domain\Username (if the Domain is required), otherwise enter the Username.
- Enter the password.

To use Automatic PAC Provisioning:

- No additional entries are required.

To use manual PAC Provisioning:

- Enter the PAC Filename and PAC Password.
- The PAC file must be copied to the directory specified in the Certs Path global variable. The PAC file must not be read only.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

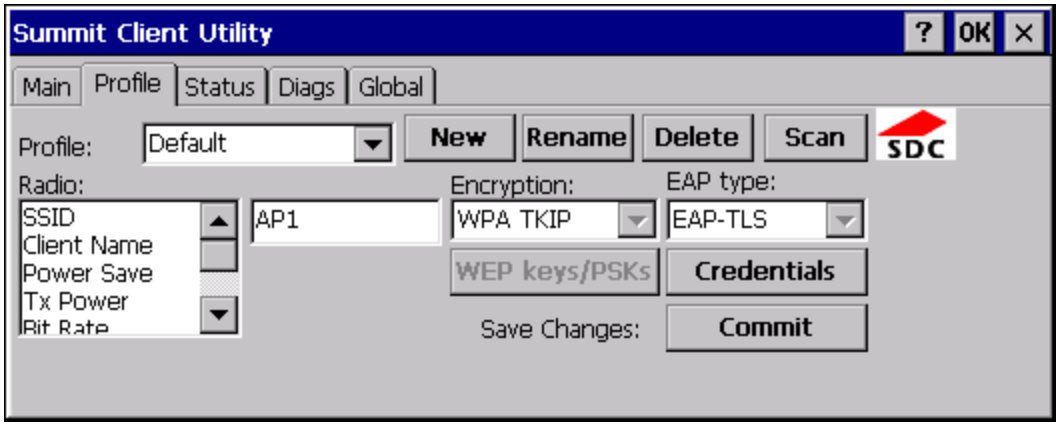
Note: When using Automatic PAC Provisioning, once authenticated, there is a file stored in the \System directory with the PAC credentials. If the username is changed, that file must be deleted. The filename is autoP.00.pac.

EAP-TLS

To use EAP-TLS, make sure the following profile options are used.

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **EAP-TLS**
- Set **Encryption** to **WPA TKIP**
- Set **Auth Type** to **Open**

To use another encryption type, select WPA CCKM, WPA2 AES or WPA2 CCKM for encryption and complete other entries as detailed in this section.

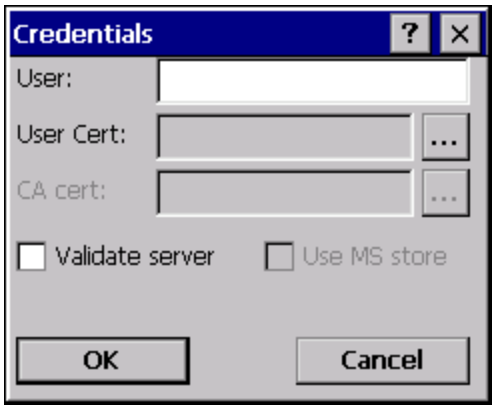


See Sign-On vs. Stored Credentials for information on entering credentials.

Click the **Credentials** button.

- No entries except the User Certificate Filename and the CA Certificate Filename are necessary for Sign-On Credentials as the user will be prompted for the User Name when connecting to the network.
- For Stored Credentials, User Certificate Filename and the CA Certificate Filename must be entered.

Enter these items as directed below.



Enter the Domain\Username (if the Domain is required), otherwise enter the Username.

Select a user certificate from the Windows certificate store. Use the **Browse** button to locate the User Cert from the certificate store. Highlight the desired certificate and press the **Select** button. The name of the certificate is displayed in the User Cert box.

Some versions of the SCU require a User Cert password. If this entry field is present, enter the password for the user certificate in the User Cert pwd box.

If there are no user certificates in the Windows certificate store, follow these instructions to generate and install the user certificate.

See Windows Certificate Store vs. Certs Path for more information on CA certificate storage.

Check the **Validate server** checkbox.

If using the Windows certificate store:

- Check the **Use MS store** checkbox. The default is to use the Full Trusted Store.
- To select an individual certificate, click on the **Browse** button.
- Uncheck the **Use full trusted store** checkbox.
- Select the desired certificate and click **Select**. You are returned to the Credentials screen.

If using the Certs Path option:

- Leave the Use MS store box unchecked.
- Enter the certificate filename in the CA Cert textbox.

Click **OK** then click **Commit**.

The VX7 should be authenticating the server certificate and using EAP-TLS for the user authentication.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

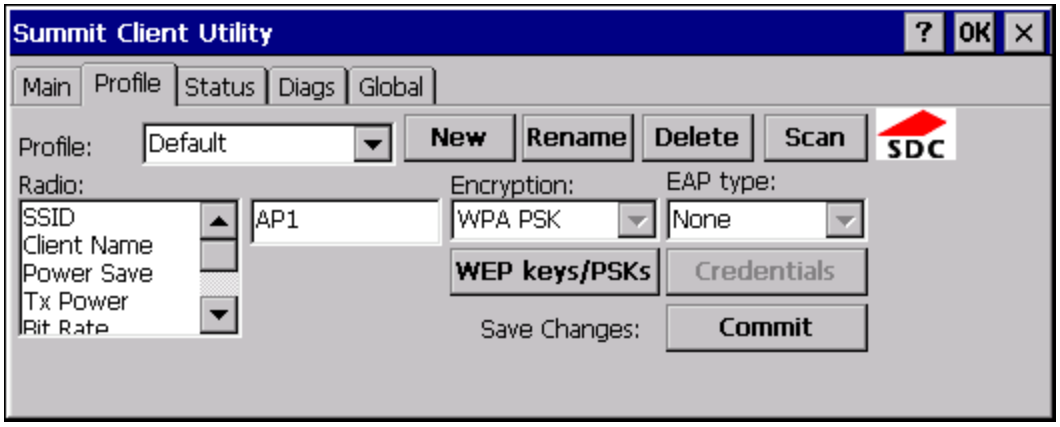
See Certificates for information on generating a Root CA certificate or a User certificate.

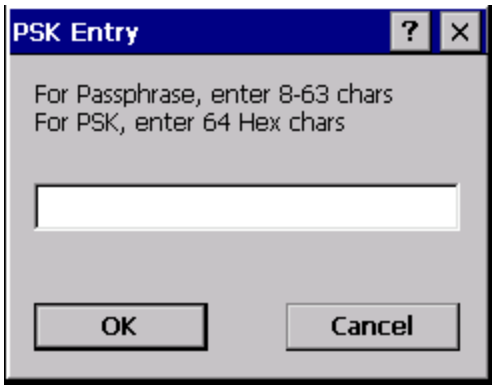
Note: The date must be properly set on the device to authenticate a certificate.

WPA PSK

To connect using WPA/PSK, make sure the following profile options are used:

- Enter the **SSID** of the Access Point assigned to this profile
- Set **EAP Type** to **None**
- Set **Encryption** to **WPA PSK** or **WPA2 PSK**
- Set **Auth Type** to **Open**





This value can be 64 hex characters or an 8 to 63 byte ASCII value. Enter the key and click **OK**.

Once configured, click the **Commit** button.

Ensure the correct Active Profile is selected on the Main tab and warmboot. The SCU Main tab shows the device is associated after the radio connects to the network.

Certificates

Note: Please refer to the Security Primer to prepare the Authentication Server and Access Point for communication.

Note: It is important that all dates are correct on the VX7 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

Quick Start

Root Certificates are necessary for EAP-TLS, PEAP/GTC and PEAP/MSCHAP.

1. Generate a Root CA Certificate and download it to a PC.
2. Connect the VX7 to the desktop PC using ActiveSync and copy the certificate to the VX7 \System folder.
3. Install the Root CA Certificate.

User Certificates are necessary for EAP-TLS

1. Generate a User Certificate and Private Key file and download it to a PC.
2. Connect the VX7 to the desktop PC using ActiveSync and copy the certificate and private key file to the VX7 \System folder.
3. Install the User Certificate and Private Key file.
4. After installation, perform a Suspend/Resume.
5. Verify installation.

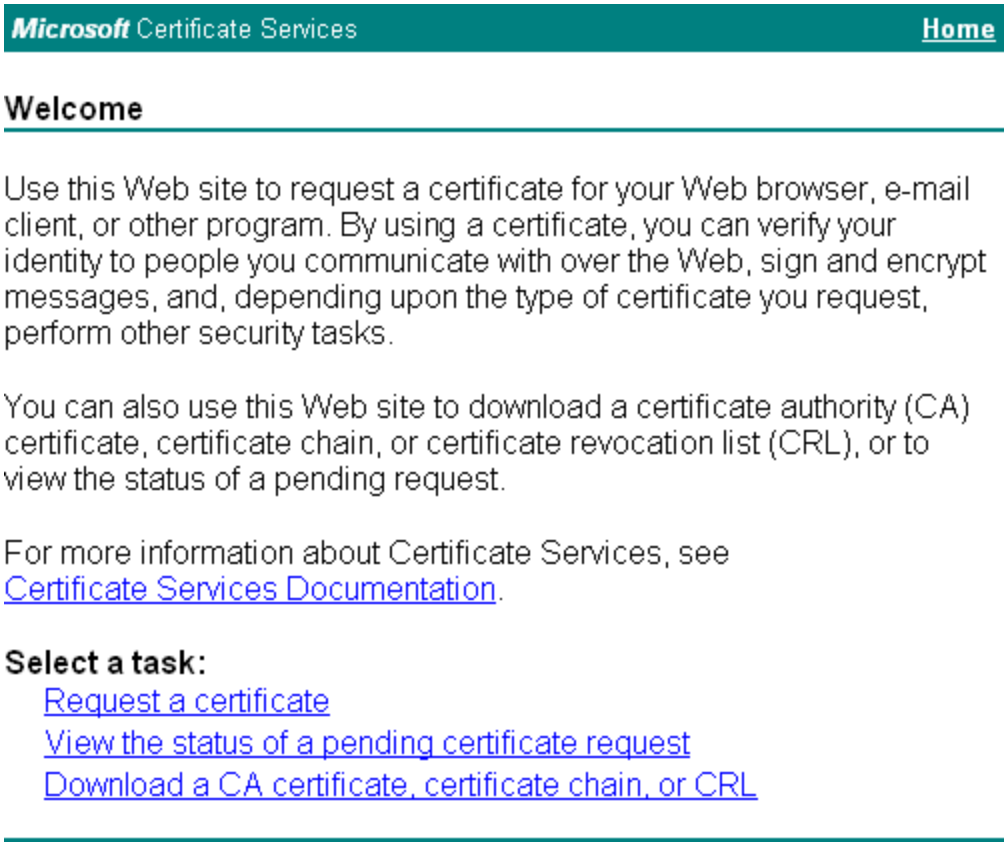
Generating a Root CA Certificate

Note: It is important that all dates are correct on the VX7 and host computers when using any type of certificate. Certificates are date sensitive and if the date is not correct authentication will fail.

The easiest way to get the root CA certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the root CA certificate, open a browser to

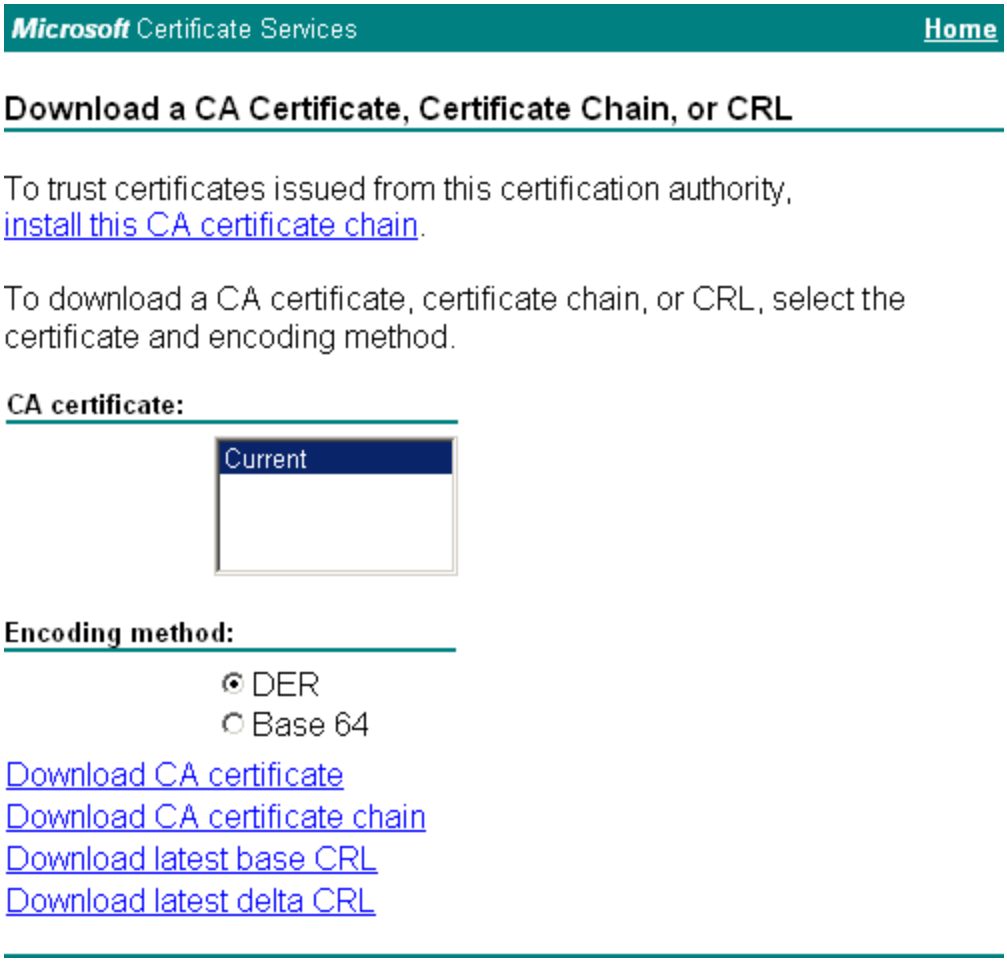
http://<CA IP address>/certsrv.

Sign into the CA with any valid username and password.


Microsoft Certificate Services
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

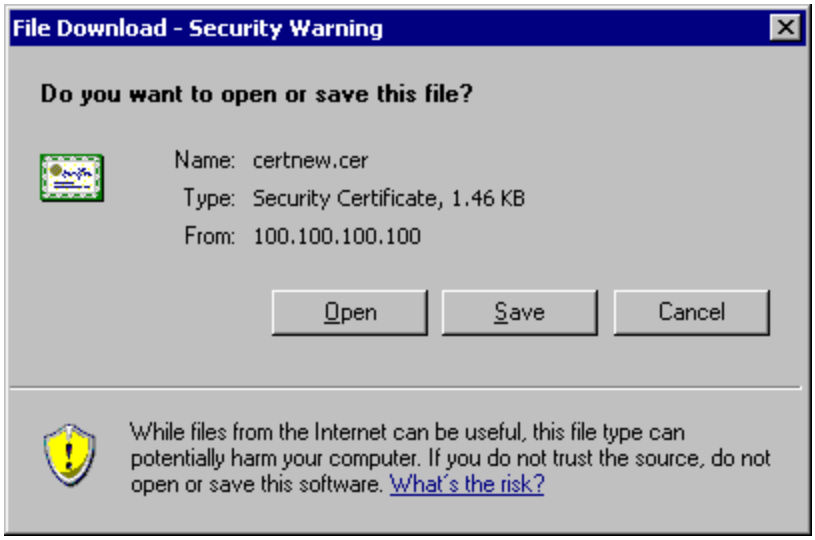
Click the **Download a CA certificate, certificate chain or CRL** link.

Make sure the correct root CA certificate is selected in the list box.


Microsoft Certificate Services
Home
Download a CA Certificate, Certificate Chain, or CRL
To trust certificates issued from this certification authority, install this CA certificate chain.
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:
Current
Encoding method:
DER
Base 64
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Click the **DER** button.

To download the CA certificate, click on the **Download CA certificate** link.


File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.46 KB
From: 100.100.100.100
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Click the **Save** button and save the certificate. Make sure to keep track of the name and location of the certificate.

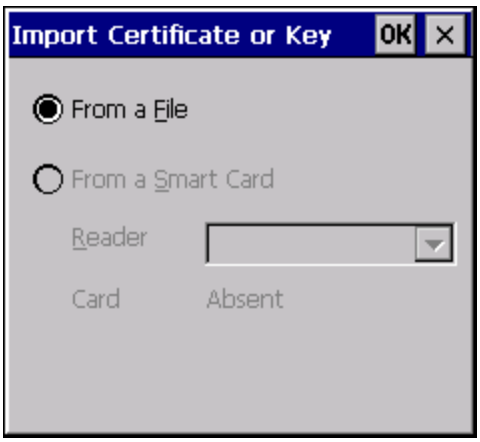
Install the certificate on the VX7.

Installing a Root CA Certificate

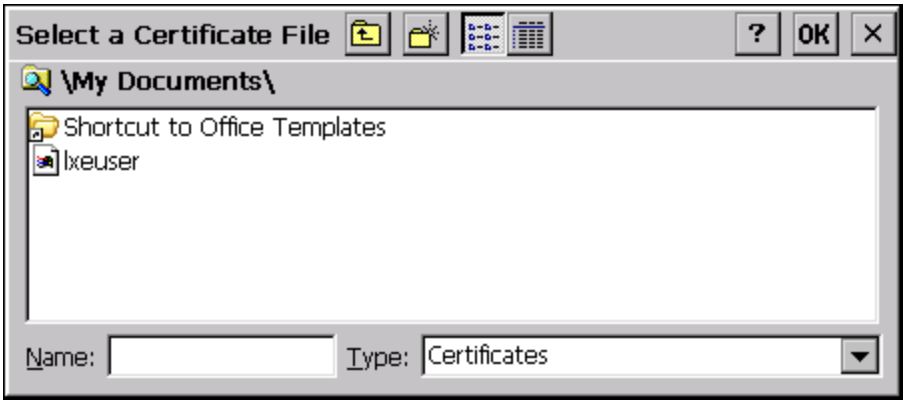
Note: This section is only if the Windows certificate store is used. If the certificate store is not used, copy the certificate to the \System folder or other path specified in the Summit Certs global parameter.

Copy the certificate file to the VX7. Import the certificate by navigating to **Start > Control Panel > Certificates**.

Tap the **Import** button.



Make sure **From a File** is selected and tap **OK**.



Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**.

Root Certificate Store
Do you want to ADD the following certificate to the Root Store?
Subject : doe, SUPPORT, LOCAL
Issuer : mickey, LOCAL
Time Validity : Thursday, July 01, 2004 through Tuesday, July 01, 2014
Serial Number : 12345678 90ABCDEF 12345678 90ABCDEF
Yes
No

Tap **Yes** to import the certificate.

Once the certificate is installed, return to the proper authentication section, earlier in this manual.

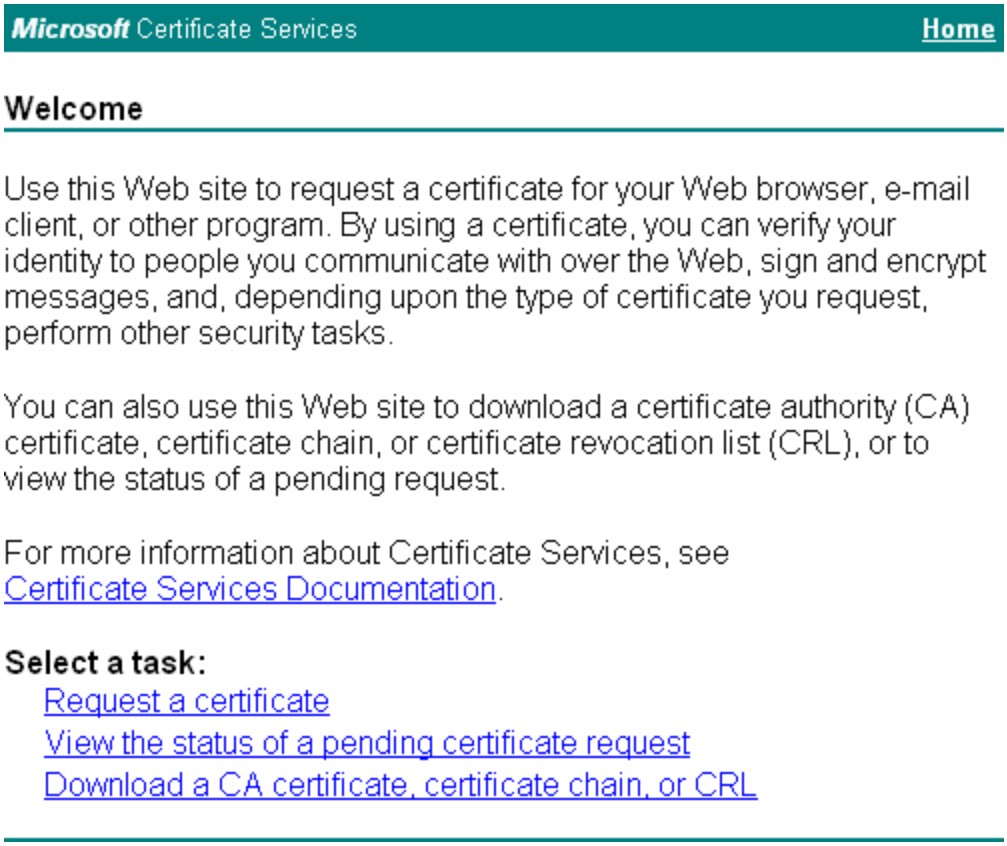
Generating a User Certificate

The easiest way to get the user certificate is to use a browser on a PC to navigate to the Certificate Authority. To request the user certificate, open a browser to

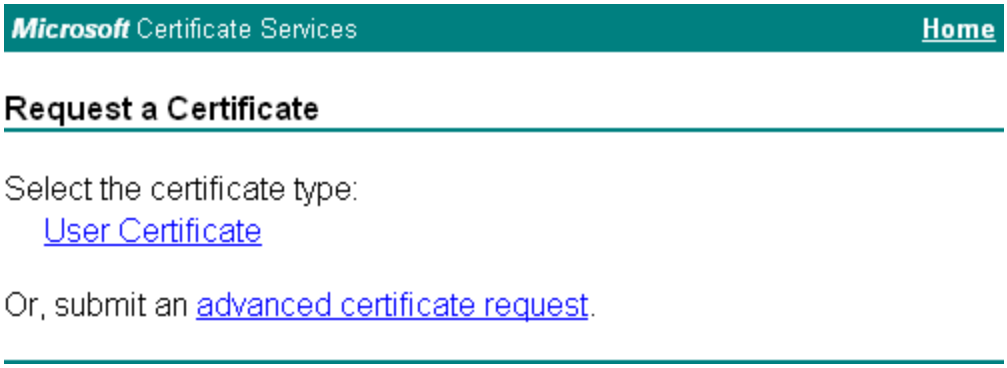
http://<CA IP address>/certsrv.

Sign into the CA with the username and password of the person who will be logging into the mobile device.

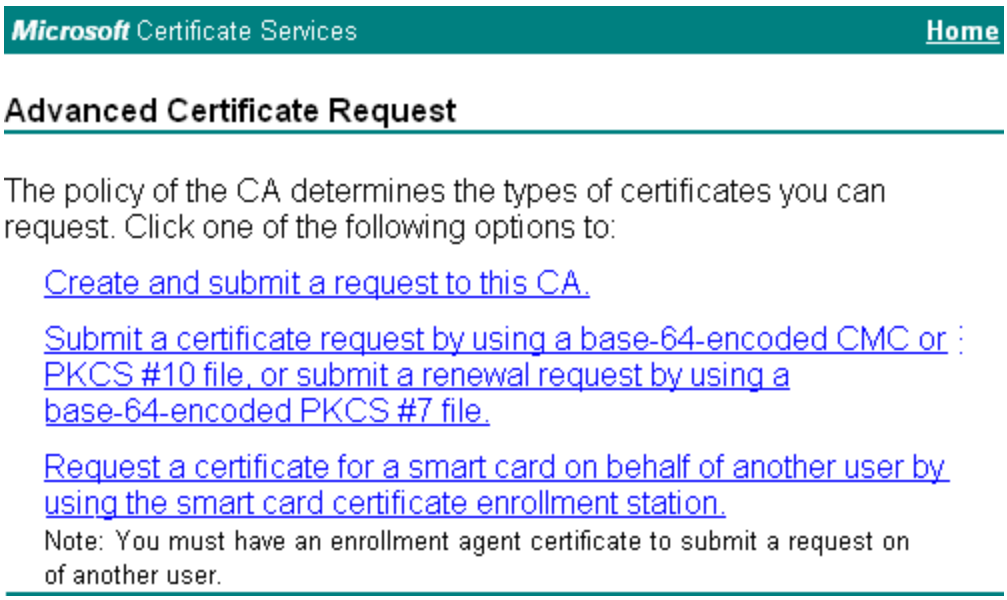
This process saves a user certificate and a separate private key file. Windows CE equipped devices such as the VX7 require the private key to be saved as a separate file rather than including the private key in the user certificate.


Microsoft Certificate Services
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Certificate Services, see Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

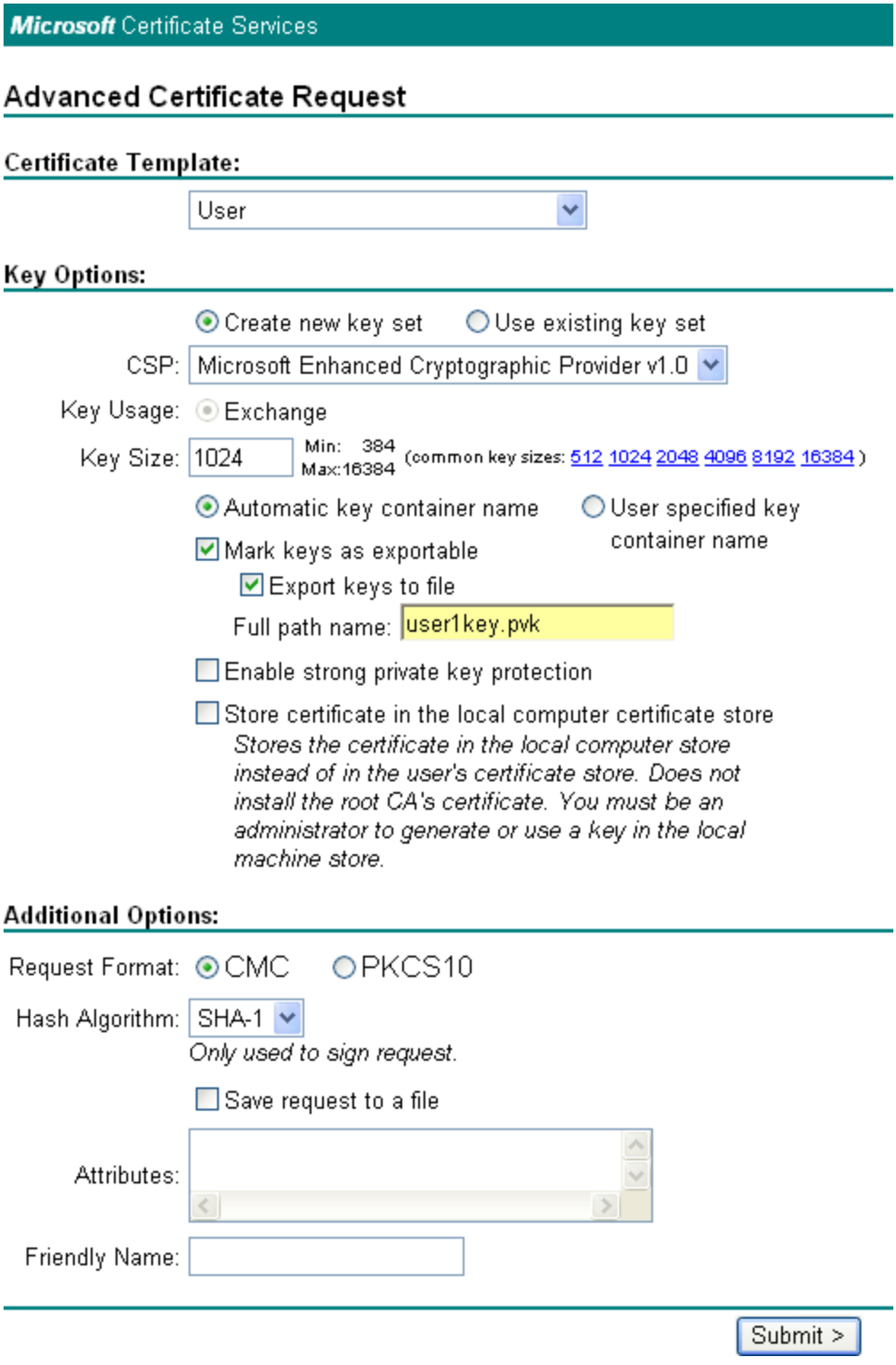
Click the **Request a certificate** link.



Click on the **advanced certificate request** link.


Microsoft Certificate Services
Home
Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.
Note: You must have an enrollment agent certificate to submit a request on of another user.

Click on the **Create and submit a request to this CA** link.



For the **Certificate Template**, select **User**.

Check the **Mark keys as exportable** and the **Export keys to file** checkboxes.

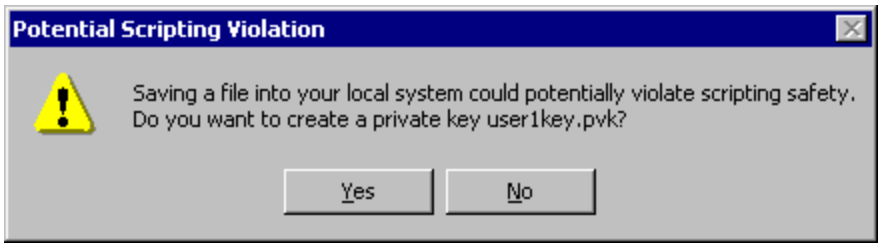
Type the full path on the local PC where the private key is to be copied. Also specify the private key filename.

Be sure to note the name used for the private key file, for example USER1.PVK. The certificate file created later in this process must be given the same name, for example, USER1.CER.

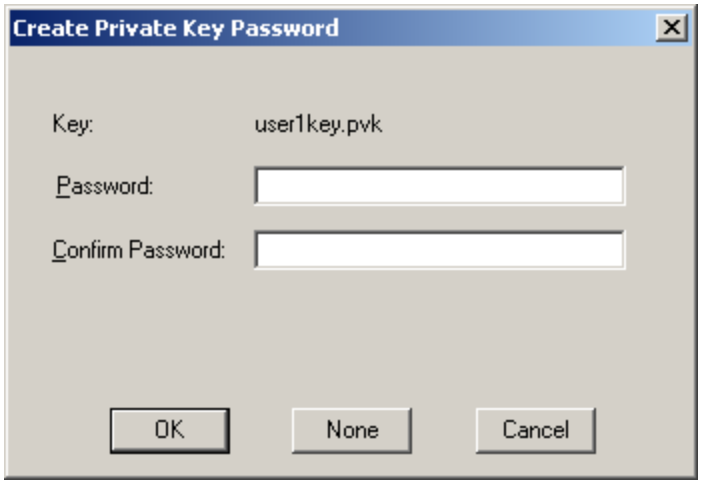
DO NOT check to use strong private key protection.

Make any other desired changes and click the **Submit** button.

Potential Scripting Violation
This Web site is requesting a new certificate on your behalf. You should allow only trusted Web sites to request a certificate for you.
Do you want to request a certificate now?
Yes
No

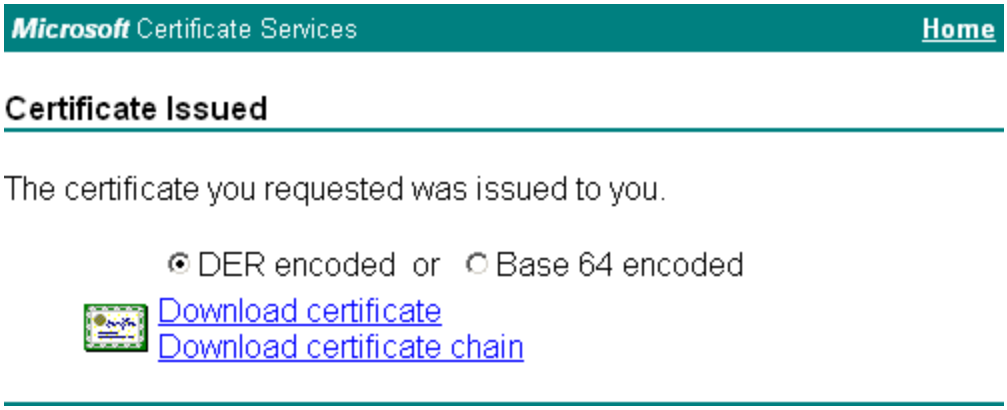

Potential Scripting Violation
Saving a file into your local system could potentially violate scripting safety.
Do you want to create a private key user1key.pvk?
Yes
No

If any script notifications occur, click the "**Yes** button to continue the certificate request.

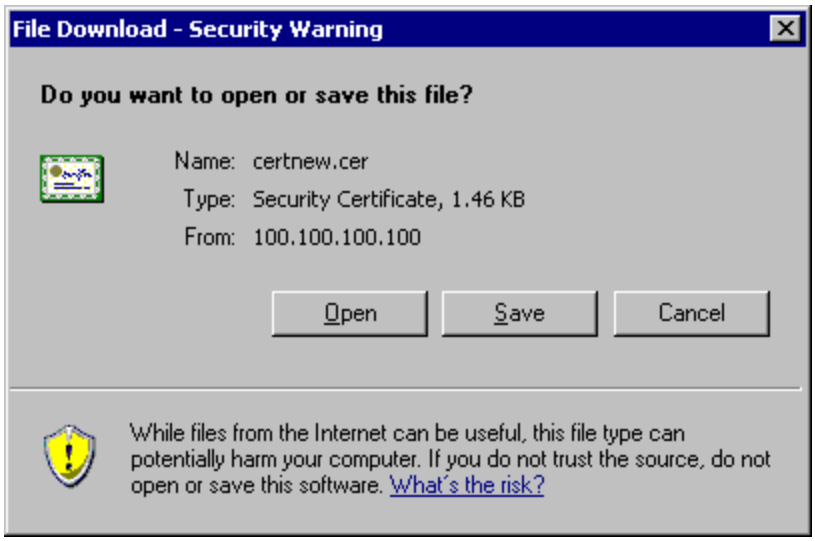


When prompted for the private key password:

- Click **None** if you do not wish to use a password, or
- Enter and confirm your desired password then click **OK**.



Click the **Download certificate** link.


File Download - Security Warning
Do you want to open or save this file?
Name: certnew.cer
Type: Security Certificate, 1.46 KB
From: 100.100.100.100
Open
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

Click **Save** to download and store the user certificate to the PC. Make sure to keep track of the name and location of the certificate. The private key file is also downloaded and saved during this process.

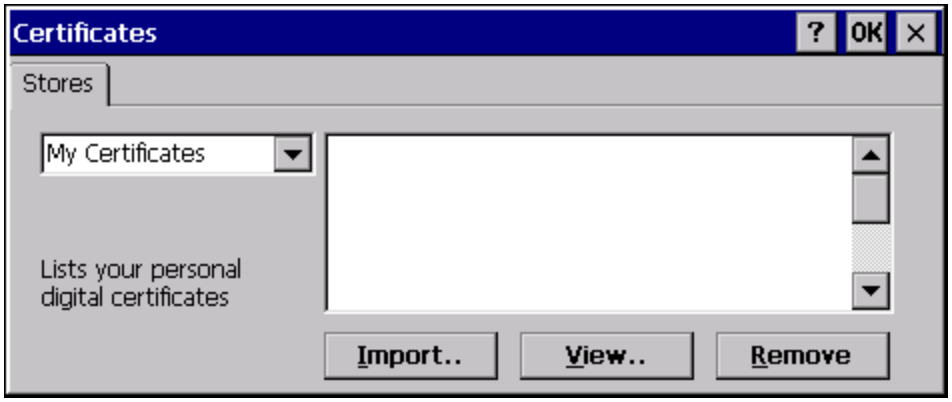
Be sure use the same name for the certificate file as was used for the private key file. For example, it the private key was saved as USER1.PVK then the certificate file created must be given the same name, for example, USER1.CER.

Install the user certificate.

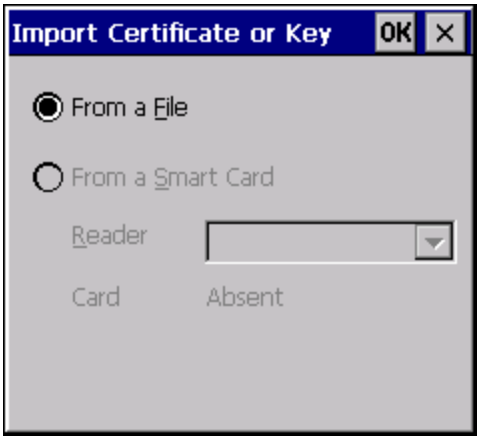
Installing a User Certificate

Copy the certificate and private key files to the VX7. Import the certificate by navigating to **Start > Control Panel > Certificates**.

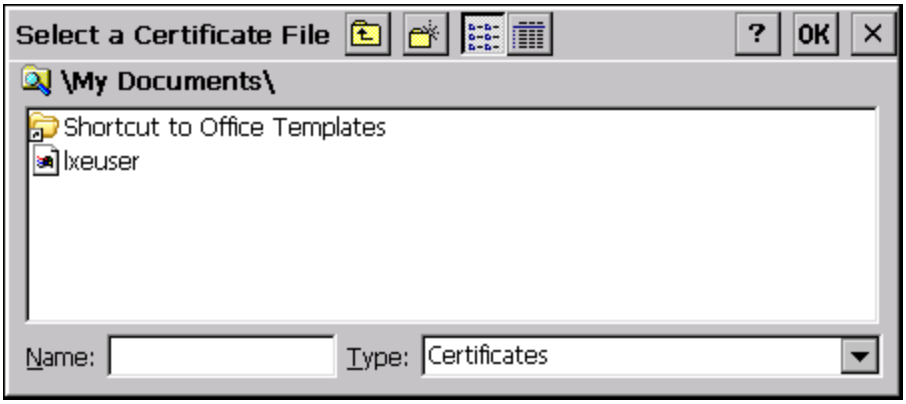
Select **My Certificates** from the pull down list.



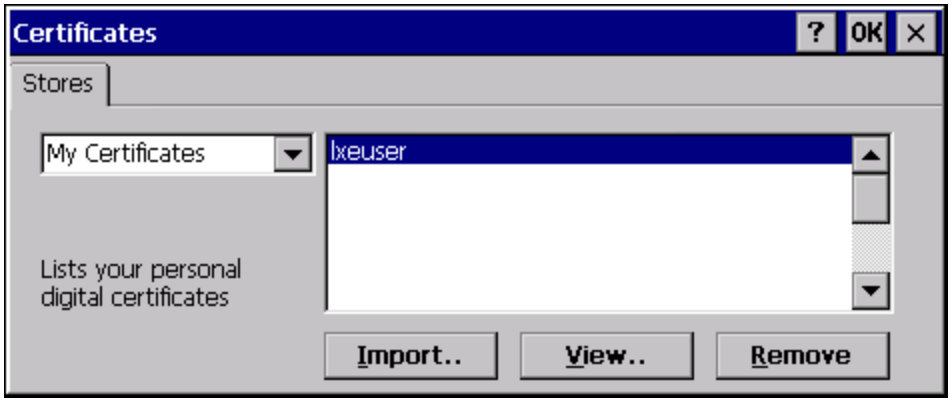
Tap the **Import** button.



Make sure **From a File** is selected and tap **OK**.

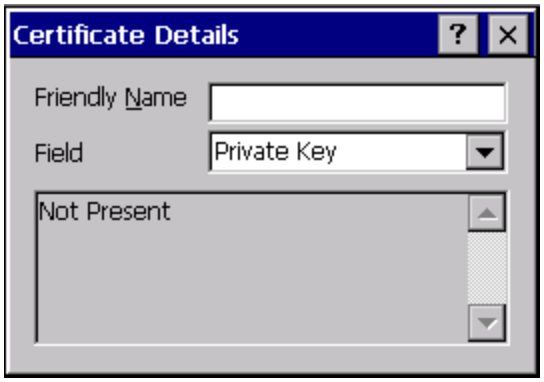


Using the explorer buttons, browse to the location where you copied the certificate, select the certificate desired and tap **OK**. The certificate is now shown in the list.



With the certificate you just imported highlighted, tap **View**.

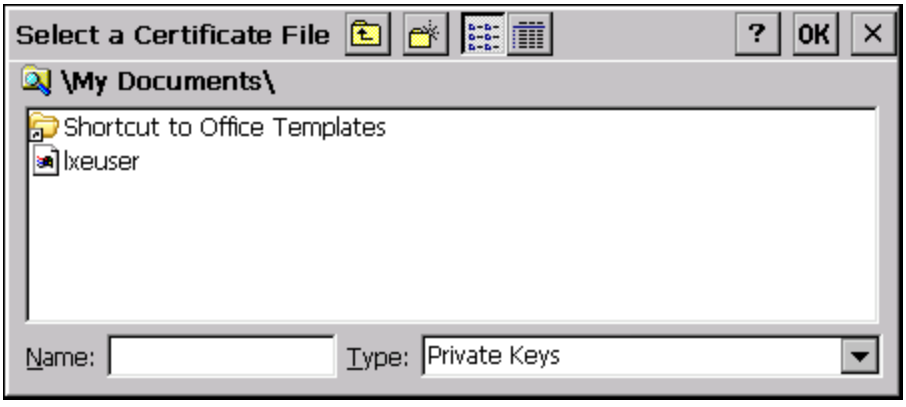
From the Field pull down menu, select **Private Key**.



- If the private key is present, the process is complete.
- If the private key is not present, import the private key.

To import the private key, tap **OK** to return to the Certificates screen.

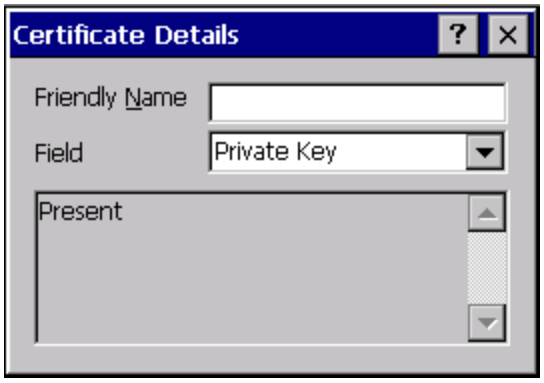
Tap import.



Using the explorer buttons, browse to the location where you copied the private key file, change the Type pull down list to **Private Keys**, select the certificate desired and tap **OK**. Enter the password for the certificate if appropriate.

Verify Installation

Tap on **View** to see the certificate details again.

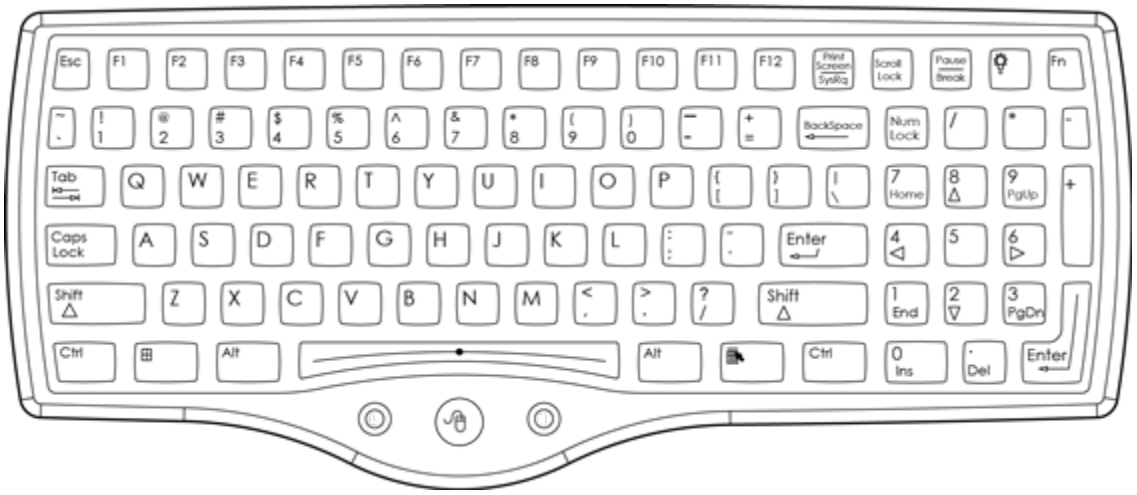


The private key should now say present. If it does not, there is a problem. Possible items to check:

- Make sure the certificate was generated with a separate private key file, as shown earlier in this section. If the certificate was not generated with a separate private key file, generate a new certificate and follow the import process again.
- Make sure the certificate and private key file have the same name, for example USER1.CER for the certificate and USER1.PVK for the private key file. If the file names are not the same, rename the private key file and import it again.

Chapter 6: Keymaps

95 Key KeyMap 101-Key Equivalencies

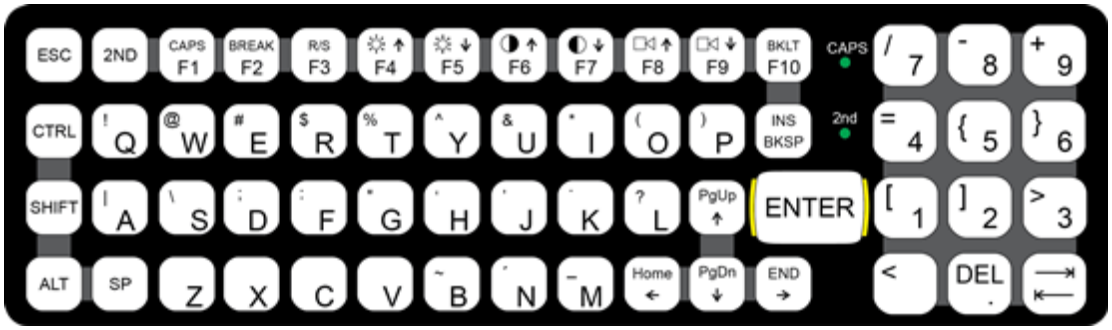


The key map table that follows lists the commands used for the VX7. Note that since the VX7uses a Microsoft Windows CE operating system, no DOS Terminal Emulation keypress sequences are provided.

There are 10 hidden keys on the 95 key keyboard. Each of the hidden keys is accessed by pressing the <Fn> key (located in the top right hand corner) plus a key on the numeric keypad on the right.

To get this Key / Function	**Press These Keys in this Order**	
Insert	FN	0 (numeric keypad)
Home	FN	7 (numeric keypad)
Page Up	FN	9 (numeric keypad)
Delete	FN	. (numeric keypad)
End	FN	1 (numeric keypad)
Page Down	FN	3 (numeric keypad)
Up Arrow	FN	8 (numeric keypad)
Left Arrow	FN	4 (numeric keypad)
Down Arrow	FN	2 (numeric keypad)
Right Arrow	FN	6 (numeric keypad)

60 Key KeyMap 101-Key Equivalencies



- The following keymap is used on a VX7 that is NOT running RFTerm. RFTerm uses a separate keymap.
- When using a sequence of keys that includes the 2nd key, press the 2nd key first then the rest of the key sequence.
- When the VX7 boots, the default condition of Caps (or CapsLock) is Off. The Caps (or CapsLock) condition can be toggled with a 2nd+F1 key sequence. The CAPS LED is illuminated when CapsLock is On. The warmboot behavior of CapsLock can be set via the Misc tab in **Start > Settings > Control Panel > MX3-VXC Options**.
- The VX7 keyboard has several control keys. The following control keys are not used:
  - The 2nd function of the **<F3>** key is not used as Windows Power Management controls all power management modes on the VX7.
  - The 2nd functions of the **<F4> and <F5>** keys are not used as the display brightness is adjusted via the buttons on the control panel.
  - The 2nd functions of the **<F6>, and <F7>** keys are not used as the VX7 has TFT LCD screen with no provision for contrast adjustments.
  - The 2nd functions of the **<F8> and <F9>** keys are not used as the sound volume on the VX7 is controlled with the Volume and Sounds icon in the Microsoft Windows CE Control Panel.
  - The 2nd function of the **<F10>** key is not used as the display backlight timer also controls the keyboard backlight.

To get this Key / Function	**Press These Keys in this Order**		
Power On/Off	Power		
2nd	2nd		
Shift	Shift		
Alt	Alt		
Ctrl	Ctrl		
Esc	Esc		
Space	Sp		
Enter	Enter		
Enter (numeric)	2nd	Enter	
CapsLock (Toggle)	2nd	F1	
Back Space	BkSp		

Tab	Tab		
Back Tab	2nd	Tab	
Ctrl-Break	Ctrl	2nd	F2
Pause	2nd	F2	
Up Arrow	Up Arrow		
Down Arrow	Down Arrow		
Right Arrow	Right Arrow		
Left Arrow	Left Arrow		
Insert	2nd	Bksp	
Delete (numeric)	2nd	DOT	
Home	2nd	Left Arrow	
End	2nd	Right Arrow	
Page Up	2nd	Up Arrow	
Page Down	2nd	Down Arrow	
ScrollLock	2nd	Shift	F10
F1	F1		
F2	F2		
F3	F3		
F4	F4		
F5	F5		
F6	F6		
F7	F7		
F8	F8		
F9	F9		
F10	F10		
F11	2nd	Shift	F1
F12	2nd	Shift	F2
a	CapsLock Off	A	
b	CapsLock Off	B	
c	CapsLock Off	C	
d	CapsLock Off	D	
e	CapsLock Off	E	
f	CapsLock Off	F	
g	CapsLock Off	G	
h	CapsLock Off	H	

i	CapsLock Off	I	
j	CapsLock Off	J	
k	CapsLock Off	K	
l	CapsLock Off	L	
m	CapsLock Off	M	
n	CapsLock Off	N	
o	CapsLock Off	O	
p	CapsLock Off	P	
q	CapsLock Off	Q	
r	CapsLock Off	R	
s	CapsLock Off	S	
t	CapsLock Off	T	
u	CapsLock Off	U	
v	CapsLock Off	V	
w	CapsLock Off	W	
x	CapsLock Off	X	
y	CapsLock Off	Y	
z	CapsLock Off	Z	
A	2nd	F1	A
B	2nd	F1	B
C	2nd	F1	C
D	2nd	F1	D
E	2nd	F1	E
F	2nd	F1	F
G	2nd	F1	G
H	2nd	F1	H
I	2nd	F1	I
J	2nd	F1	J
K	2nd	F1	K
L	2nd	F1	L
M	2nd	F1	M
N	2nd	F1	N
O	2nd	F1	O
P	2nd	F1	P
Q	2nd	F1	Q

R	2nd	F1	R
S	2nd	F1	S
T	2nd	F1	T
U	2nd	F1	U
V	2nd	F1	V
W	2nd	F1	W
X	2nd	F1	X
Y	2nd	F1	Y
Z	2nd	F1	Z
1	1		
2	2		
3	3		
4	4		
5	5		
6	6		
7	7		
8	8		
9	9		
0	0		
DOT	DOT		
<	2nd	0	
[	2nd	1	
]	2nd	2	
>	2nd	3	
=	2nd	4	
{	2nd	5	
}	2nd	6	
/ (numeric)	2nd	Ctrl	7
/ (alpha)	2nd	7	
- (numeric)	2nd	Ctrl	8
- (alpha)	2nd	8	
+ (numeric)	2nd	Ctrl	9
+ (alpha)	2nd	9	
* (numeric)	2nd	l (letter i)	
* (alpha)	2nd	Ctrl	l (letter i)

: (colon)	2nd	D	
; (semicolon)	2nd	F	
?	2nd	L	
`	2nd	N	
_ (underscore)	2nd	M	
, (comma)	2nd	J	
' (apostrophe)	2nd	H	
~ (tilde)	2nd	B	
\	2nd	S	
|	2nd	A	
"	2nd	G	
!	2nd	Q	
@	2nd	W	
#	2nd	E	
$	2nd	R	
%	2nd	T	
^	2nd	Y	
&	2nd	U	
(	2nd	O	
)	2nd	P	

IBM Terminal Emulation

The VX7's IBM 3270 and IBM 5250 Terminal Emulator keypads are designed to allow the user to enter terminal emulator commands when running RFTerm. When running RFTerm on the VX7, please refer to RFTerm documentation for equivalent keys and keypress sequences.

IBM 3270

Legend on Keypad	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
E-Inp	Erase Input	Ctrl + BkSp
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
PA1		Ctrl + F1
PA2		Ctrl + F2
PA3		Ctrl + F3
Rst	Reset	Ctrl + R
SysReq	System	Ctrl + S

IBM 5250

Legend on Keypad	Explanation	Key Sequence
Attn	Attention	Ctrl + A
Clr	Clear	Ctrl + C
Del	Delete	Ctrl + D
Dup	Duplicate	Ctrl + U
E-Inp	Erase Input	Ctrl + Bksp
Field Exit	Enter	Enter
Fld -	Field Minus	Ctrl + M
Fld +	Field Plus	Ctrl + L
Ins	Insert	Ctrl + I
NL	New Line	Ctrl + N
SysReq	System	Ctrl + S

Chapter 7: Technical Specifications

VX7

Processor	XScale PXA255 CPU operating at 400 MHz
Memory	RAM: 128MB SDRAM / ROM: 128MB flash
Mass Storage	CompactFlash/Secure Digital/PCMCIA (Depending on configuration ordered)
Operating System	Microsoft Windows CE 5.0
Radio Modules	802.11 b/g or a/b/g radio, Bluetooth
Scanner options	No integrated scanner
Display technology	Controller: SVGA compatible controller Type: TFT Full Screen Resolution: Default is 800 X 600 pixels (25 lines x 80 characters) Resolution: Optional - 640x480 pixels Cell Size: 8 x 16 pixels (8 x 8 also supported – 25 lines x 80 chars) Dot Dimensions: .30mm x .30mm Display Dimensions: 280mm x 218mm x 11mm (11.0” x 8.6” x 0.4”) Viewing Area: 249mm x 187.5mm (9.8” x 7.38”) Active Display Area: 246mm x 98.3mm (9.7” x 3.87”) 350 NIT (indoor) or 500 NIT (outdoor) brightness display
External Connectors	Two external RS-232C serial ports, COM1 and COM3, with switchable power Keyboard/mouse connector 2.5mm audio/microphone jack USB Client Port and USB Host Port via adapter cable Optional Ethernet port via adapter cable Optional single or dual external 802.11 antenna connectors
PCMCIA/CardBus Interface	Two (2) PCMCIA: Accepts Type I and II PCMCIA cards
Power Connector	5-pin connector. 12-80V DC input power
Power Switch	Sealed power switch
Beeper	Minimum loudness greater than 95dBm at 10 cm in front of unit
External Power Supply	External power supply, AC Adapter, 120-240VAC to 12VDC
Backup Battery (CMOS)	Internal lithium Battery
Input Power	DC Input Voltage: 12 - 80 VDC Input Current: 1.25 Amps Input Fuse: 2A Time Delay

Dimensions

Length	12.2” (30.98 cm)
Width	9.6” (24.38 cm)
Height	3.7” (9.39 cm)

Environmental Specifications

VX7

Operating Temperature	Standard: -4°F to 122°F (-20°C to 50°C) [non-condensing] Extended temperature: -22º to 122º F (-30ºC to 50ºC) [condensing]
Storage Temperature	Standard and Extended temperature: -22°F to 140°F (-30°C to 60°C) [non-condensing]
ESD	8 KV air, 4kV direct contact
Operating Humidity	Standard: Up to 90% non-condensing at 104°F (40°C) Extended temperature: 100%
Water and Dust	IEC 60529 compliant to IP66
ESD	15 kV
Vibration	Bounce loose cargo for 0.5 hour duration. Common carrier transportation, transit face
Altitude	Operational to 10,000 ft. (3048 meters)

UPS Battery Pack

Operating Temperature	-30 °C to +50 °C (-22 °F to +122 °F)
Storage Temperature	-40 °C to +70 °C (-40 °F to +158 °F)
Operating Humidity	10% to 90% non-condensing at 104°F (40°C)
Water and Dust	IEC 60529 compliant to IP66
ESD	15 kV
Vibration	Bounce loose cargo for 0.5 hour duration. Common carrier transportation, transit face
Altitude	Operational to 10,000 ft. (3048 meters)

Network Card Specifications

Summit 802.11 b/g CF 2.4GHz

Bus Interface	16-bit CompactFlash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	50 mW max.
Channels	1-11 FCC, 1-13 ETSI
Operating Temperature	Same as VX7 Operating Temperature
Storage Temperature	Same as VX7 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Summit 802.11a/b/g CF 2.4/5.0GHz

Bus Interface	16-bit CompactFlash Type I with 50-pin connector
Wireless Frequencies	2.4 to 2.4897 GHz IEEE 802.11b / 802.11g DSSS OFDM 5.0GHz IEEE 802.11a DSSS OFDM
RF Data Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
RF Power Level	64 mW (18dBm)
Channels	FCC: 1-11, 36, 40 ,44, 48, 149, 153, 157, 161 ETSI: 1-13, 36, 40, 44 ,48
Operating Temperature	Same as VX7 Operating Temperature
Storage Temperature	Same as VX7 Storage Temperature
Connectivity	TCP/IP, Ethernet, ODI
Diversity	Yes

Bluetooth

Bus Interface	CompactFlash
Enhanced Data Rate	Up to 3.0 Mbit/s over the air
Connection	No less than 32.80 feet (10 meters) line of sight
Bluetooth Version	2.0 + EDR
Operating Frequency	2.402 - 2.480 GHz
QDID	B013455

Chapter 8: Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Product Service and Repair

Honeywell International Inc. provides service for all of its products through service centers throughout the world. To obtain warranty or non-warranty service, please visit www.honeywellaidc.com and select **Support > Contact Service and Repair** to see your region's instructions on how to obtain a Return Material Authorization number (RMA #). You should do this prior to returning the product.

Limited Warranty

Honeywell International Inc. ("HII") warrants its products to be free from defects in materials and workmanship and to conform to HII's published specifications applicable to the products purchased at the time of shipment. This warranty does not cover any HII product which is (i) improperly installed or used; (ii) damaged by accident or negligence, including failure to follow the proper maintenance, service, and cleaning schedule; or (iii) damaged as a result of (A) modification or alteration by the purchaser or other party, (B) excessive voltage or current supplied to or drawn from the interface connections, (C) static electricity or electro-static discharge, (D) operation under conditions beyond the specified operating parameters, or (E) repair or service of the product by anyone other than HII or its authorized representatives.

This warranty shall extend from the time of shipment for the duration published by HII for the product at the time of purchase ("Warranty Period"). Any defective product must be returned (at purchaser's expense) during the Warranty Period to HII factory or authorized service center for inspection. No product will be accepted by HII without a Return Materials Authorization, which may be obtained by contacting HII. In the event that the product is returned to HII or its authorized service center within the Warranty Period and HII determines to its satisfaction that the product is defective due to defects in materials or workmanship, HII, at its sole option, will either repair or replace the product without charge, except for return shipping to HII.

EXCEPT AS MAY BE OTHERWISE PROVIDED BY APPLICABLE LAW, THE FOREGOING WARRANTY IS IN LIEU OF ALL OTHER COVENANTS OR WARRANTIES, EITHER EXPRESSED OR IMPLIED, ORAL OR WRITTEN, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

HII'S RESPONSIBILITY AND PURCHASER'S EXCLUSIVE REMEDY UNDER THIS WARRANTY IS LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT WITH NEW OR REFURBISHED PARTS. IN NO EVENT

SHALL HII BE LIABLE FOR INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, AND, IN NO EVENT, SHALL ANY LIABILITY OF HII ARISING IN CONNECTION WITH ANY PRODUCT SOLD HEREUNDER (WHETHER SUCH LIABILITY ARISES FROM A CLAIM BASED ON CONTRACT, WARRANTY, TORT, OR OTHERWISE) EXCEED THE ACTUAL AMOUNT PAID TO HII FOR THE PRODUCT. THESE LIMITATIONS ON LIABILITY SHALL REMAIN IN FULL FORCE AND EFFECT EVEN WHEN HII MAY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH INJURIES, LOSSES, OR DAMAGES. SOME STATES, PROVINCES, OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATIONS OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

All provisions of this Limited Warranty are separate and severable, which means that if any provision is held invalid and unenforceable, such determination shall not affect the validity of enforceability of the other provisions hereof. Use of any peripherals not provided by the manufacturer may result in damage not covered by this warranty. This includes but is not limited to: cables, power supplies, cradles, and docking stations. HII extends these warranties only to the first end-users of the products. These warranties are non-transferable.

The duration of the limited warranty for the VX7 is 1 year.

The duration of the limited warranty for the VX7 Vehicle Mount Assembly is 1 year.

The duration of the limited warranty for the VX7 external UPS battery is 1 year.

The duration of the limited warranty for the VX7 AC power supply and cables is 1 year.

The duration of the limited warranty for the VX7 DC-DC Converter is 1 year.

The duration of the limited warranty for the VX7 cables (USB, Serial, Communication, Power) is 1 year.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707
www.honeywellaidc.com

E-EQ-VX6RG
Rev AA
10/12